Union Calendar No. 84

93d Congress, 1st Session - - - - - - House Report No. 93-221

EXECUTIVE CLASSIFICATION OF INFORMATION—SECURITY CLASSIFICATION PROBLEMS INVOLVING EXEMPTION (b)(1) OF THE FREEDOM OF INFORMATION ACT (5 U.S.C. 552)

THIRD REPORT

BY THE

COMMITTEE ON GOVERNMENT OPERATIONS

MAY 22, 1973.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

U.S. GOVERNMENT PRINTING OFFICE

95-679 O WASHINGTON : 1973

COMMITTEE ON GOVERNMENT OPERATIONS

CHET HOLIFIELD, California, *Chairman*

JACK BROOKS, Texas
L. H. FOUNTAIN, North Carolina
ROBERT E. JONES, Alabama
JOHN E. MOSS, California
DANTE B. FASCELL, Florida
HENRY S. REUSS, Wisconsin
TORBERT H. MACDONALD, Massachusetts
WILLIAM S. MOORHEAD, Pennsylvania
WM. J. RANDALL, Missouri
BENJAMIN S. ROSENTHAL, New York
JIM WRIGHT, Texas
FERNAND J. ST GERMAIN, Rhode Island
JOHN C. CULVER, Iowa
FLOYD V. HICKS, Washington
DON FUQUA, Florida
JOHN CONYERS, JR., Michigan
BILL ALEXANDER, Arkansas
BELLA S. ABZUG, New York
HAROLD D. DONOHUE, Massachusetts
JAMES V. STANTON, Ohio
LEO J. RYAN, California

FRANK HORTON, New York
JOHN N. ERLENBORN, Illinois
JOHN W. WYDLER, New York
CLARENCE J. BROWN, Ohio
GUY VANDER JAGT, Michigan
GILBERT GUDE, Maryland
PAUL N. McCLOSKEY, JR., California
JOHN H. BUCHANAN, JR., Alabama
SAM STEIGER, Arizona
GARRY BROWN, Michigan
CHARLES THONE, Nebraska
RICHARD W. MALLARY, Vermont
STANFORD E. PARRIS, Virginia
RALPH S. REGULA, Ohio
ANDREW J. HINSHAW, California
ALAN STEELMAN, Texas
JOEL PRITCHARD, Washington
ROBERT P. HANRAHAN, Illinois

HERBERT ROBACK, *Staff Director*
ELMER W. HENDERSON, *General Counsel*
MILES Q. ROMNEY, *Counsel-Administrator*
J. P. CARLSON, *Minority Counsel*
WILLIAM H. COPENHAVER, *Minority Professional Staff*

FOREIGN OPERATIONS AND GOVERNMENT INFORMATION SUBCOMMITTEE

WILLIAM S. MOORHEAD, Pennsylvania, *Chairman*

JOHN E. MOSS, California
TORBERT H. MACDONALD, Massachusetts
JIM WRIGHT, Texas
BILL ALEXANDER, Arkansas
BELLA S. ABZUG, New York
JAMES V. STANTON, Ohio

JOHN N. ERLENBORN, Illinois
PAUL N. McCLOSKEY, JR., California
GILBERT GUDE, Maryland
CHARLES THONE, Nebraska
RALPH S. REGULA, Ohio

EX OFFICIO

CHET HOLIFIELD, California
FRANK HORTON, New York

WILLIAM G. PHILLIPS, *Staff Director*
NORMAN G. CORNISH, *Deputy Staff Director*
HAROLD F. WHITTINGTON, *Professional Staff Member*
L. JAMES KRONFELD, *Counsel*
MARTHA M. DOTY, *Clerk*
ALMEDA J. HARLEY, *Secretary*

LETTER OF TRANSMITTAL

HOUSE OF REPRESENTATIVES,
Washington, D.C., May 22, 1973.

Hon. CARL ALBERT,
Speaker of the House of Representatives,
Washington, D.C.

DEAR MR. SPEAKER: By direction of the Committee on Government Operations, I submit herewith the committee's third report to the 93d Congress. The committee's report is based on a study made by its Foreign Operations and Government Information Subcommittee.

CHET HOLIFIELD, *Chairman.*

CONTENTS

Union Calendar No. 84

93D CONGRESS, 1st Session } HOUSE OF REPRESENTATIVES { REPORT No. 93-221

EXECUTIVE CLASSIFICATION OF INFORMATION—SECURITY CLASSIFICATION PROBLEMS INVOLVING EXEMPTION (b)(1) OF THE FREEDOM OF INFORMATION ACT (5 U.S.C. 552)

MAY 22, 1973.—Committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

Mr. HOLIFIELD, from the Committee on Government Operations, submitted the following

THIRD REPORT

BASED ON A STUDY BY THE FOREIGN OPERATIONS AND GOVERNMENT INFORMATION SUBCOMMITTEE

On May 22, 1973, the Committee on Government Operations approved and adopted a report entitled "Executive Classification of Information—Security Classification Problems Involving Exemption (b)(1) of the Freedom of Information Act (5 U.S.C. 552)." The chairman was directed to transmit a copy to the Speaker of the House.

PREFACE

This report is based on 13 days of hearings by the Foreign Operations and Government Information Subcommittee in the 92d Congress during June and July 1971, and May 1972.[1] It also incorporates the results of staff and General Accounting Office investigations and studies of the subject areas of the classification system as it has operated under Executive Order 10501 of November 9, 1953, and Executive Order 11652 of March 8, 1972. Finally, it provides a historical perspective on the classification system by summarizing major findings, recommendations, and other studies undertaken by the former Special Subcommittee on Government Information of this committee during the period 1955–62.

[1] Hearings, Foreign Operations and Government Information Subcommittee, "U.S. Government Information Policies and Practices—The Pentagon Papers," pts. 1, 2, 3, June 23, 24, 25, 28, 29, 30, and July 7, 1971; "U.S. Government Information Policies and Practices—Security Classification Problems Involving Subsection (b)(1) of the Freedom of Information Act," pt. 7, May 1, 2, 3, 5, 8, and 11, 1972.

It should be noted that this report does not include matters related to the issue of "executive privilege," nor any of the events which have transpired during the first 4 months of 1973 regarding efforts of the Nixon administration to expand that claim. This subject will be dealt with in a subsequent report of this committee.

Nor does this report deal with proposals advanced by the Justice Department in March 1973, contained in legislation to revise the Criminal Code—title 18—that would impose more stringent criminal penalties on the disclosure of information which bears classification markings.

I. INTRODUCTION

From the earliest days of our Republic the President in carrying out the provisions of article II, section 2 of the Constitution as the Commander in Chief, has limited the dissemination of information affecting our defense and foreign policy interests. Moreover, the 1789 "housekeeping" statute until amended by Congress in 1958, was utilized to withhold information from the public on a wide range of government actions—including and extending beyond information that might be related to our defense and foreign policy interests.[2]

However, the constitutional prerogative of "secrecy" is limited to "each House" of Congress as it applies to the "Journal of its Proceedings." [3] Nowhere in the Constitution or any of its amendments is there any express basis for "secrecy" as applied to activities of the executive or judicial branches of government.

The first instance of the use of article II, section 5 authority to effect secrecy was in 1790 when President Washington presented to the Senate for its approval a secret article to be inserted into a treaty with the Creek Indians.[4] Controversy arose in Congress over secret reports made in connection with General St. Clair's campaign in 1791 against the Indians on our northwest frontier and with the secret negotiations between Chief Justice John Jay and Lord Grenville that produced Jay's Treaty with Great Britain. One authority on the history of classification markings has traced such labels as "Secret," "Confidential," or "Private" on communications from military, naval, or other public officials back almost continuously for more than a century.[5]

Thus, the historical review of the confidential treatment of certain defense and foreign policy records and documents shows that, to some degree, secrecy in military and diplomatic affairs has always been practiced by the executive branch, although a formal classification system to protect such types of information did not develop until more recent times.

[2] Public Law 85-619, revising revised statutes 161. This is now codified as 5 U.S.C. 301. See H. Rept. 1461, 85th Cong., 2d sess., and hearings by Special Subcommittee on Government Information on H.R. 2767 for examples. See also 1955 hearings by this same subcommittee and H. Rept. 2947, 84th Cong., 2d sess., for additional background.

[3] Art. 1, sec. 5, clause 5.

[4] U.S. Congress, Senate, Executive Journal, vol. I, p. 55 (Aug. 4, 1790).

[5] National Archives, "Origin of Defense-Information Markings in the Army and Former War Department," prepared by Dallas Irvine, Dec. 23, 1964 (revised 1972). Most other historical examples cited below are all taken from this study.

II. HISTORICAL BACKGROUND

The origins of the present security classification system can be traced just prior to the World War I period. On February 16, 1912, a general order was issued by the War Department that established a system for protecting information relating to submarine mine projects, land defense plans, maps and charts showing locations of defense elements and the character of the armament, and data on the number of guns and supply ammunition. The order, however, prescribed no particular security markings.[6]

More than 5 years later, after the United States had entered the war, the General Headquarters of the American Expeditionary Forces published General Orders No. 64 on November 21, 1917, establishing the classifications of "Confidential," "Secret," and "For Official Circulation Only." [7] Limitations on reproduction and distribution were also provided. The system was patterned after British and French procedures.

Soon thereafter, the War Department issued more precise definitions of "Secret," "Confidential," and "For Official Use Only" in its "Changes in Compilation of Orders No. 6" on December 14, 1917.[8] Citations were also made in the order to punishment for failure to protect such information under provisions of the Articles of War or under section 1, title 1 of the Espionage Act, which had become law on June 15, 1917. Irvine notes in his study: [9]

> * * * We may surmise that invocation of the Espionage Act of 1917 was considered advisable because so many officers of the war-time army were drawn from civilian life and therefore would not have the instincts of professionals. There is no indication that there was any realization at this time that difficulties could arise in enforcing the Espionage Act if official information relating to the national defense was not marked as such, insofar as it was intended to be protected from unauthorized dissemination. * * *

The Navy Department issued General Order No. 370 on February 20, 1918, establishing and describing three "classes of correspondence and information"—"Secret," "Confidential," and "Nonconfidential." [10]

Several years after the end of World War I, the security classification system was formally continued by Army Regulation 330–5, published on January 22, 1921. The three levels of classification markings were described as follows: [11]

[6] Ibid., pp. 9–10. See also pp. 1–16 for a summary of the historical development of the security protection of vital defense information during this period.
[7] Ibid., p. 24; for a valuable background discussion of government censorship in World Wars I and II, see section of the Report of the Commission on Government Security (Wright Commission), issued in 1957, pp. 152–154; see also pp. 19–20 of this report.
[8] Ibid., pp. 26–28.
[9] Ibid., p. 31.
[10] Ibid., p. 43; see also annex T of the same study.
[11] National Archives study, op. cit., pp. 33–34.

> A document will be marked "Secret" only when the information it contains is of great importance and when the safeguarding of that information from actual or potential enemies is of prime necessity.
>
> * * * * *
>
> A document will be marked "Confidential" when it is of less importance and of less secret a nature than one requiring the mark of "Secret" but which must, nevertheless, be guarded from hostile or indiscrete persons.
>
> * * * * *
>
> A document will be marked "For official use only" when it contains information which is not to be communicated to the public or to the press but which may be communicated to any persons known to be in the service of the United States whose duty it concerns, or to persons of undoubted loyalty and discretion who are cooperating with Government work.

A noteworthy fact is that these regulations failed to relate to provisions of the Espionage Act of 1917 or to limit their application to defense information.

A subsequent revision of the regulation in 1935 added the term "Restricted," to be used when a document contained information regarding research work on the "design, test, production, or use of a unit of military equipment or a component thereof which was to be kept secret." Documents on projects with "restricted" status were to be marked as follows:[12]

> Restricted; Notice—This document contains information affecting the national defense of the United States within the meaning of the Espionage Act (U.S.C. 50:31, 32). The transmission of this document or the revelation of its contents in any manner to any unauthorized person is prohibited.

A February 11, 1936, revision of Army Regulations 330–5 dropped the marking "For Official Use Only" and redefined "Secret," "Confidential," and "Restricted" to bring them more into line with similar Navy regulations. The definition of "Secret" was as follows:[13]

> A document will be classified and marked "Secret" only when the information it contains is of such nature that its disclosure might endanger the national security, or cause serious injury to the interests or prestige of the Nation, an individual, or any government activity, or be of great advantage to a foreign nation.

[12] Ibid., pp. 38–39, change in Army Regulation 330–5; also incorporated in Change No. 3 in Army Regulations No. 850–25, Feb. 12, 1935. This was apparently the first action that linked the 1917 Espionage Act to the security classification system; see ibid., pp. 42–44 for a discussion of this point.

[13] Ibid., pp. 38–39.

"Confidential" was defined thus:

> A document will be classified and marked "Confidential" when the information it contains is of such a nature that its disclosure, although not endangering the national security, might be prejudicial to the interests or prestige of the Nation, an individual, or any government activity, or be of advantage to a foreign nation.

"Restricted" documents were given the following definition:

> A document will be classified and marked "Restricted" when the information it contains is for official use only or of such a nature that its disclosure should be limited for reasons of administrative privacy, or should be denied the general public.

Archivist historian Irvine observed: [14]

> In clearly extending the applicability of protective markings to "nondefense" information the 1936 revision of Army Regulations 330–5 contrasted with earlier versions of the same regulations, which had evaded facing up to this question of applicability. On what basis the regulations were now given their extended applicability is not made plain. The effect was to apply the menace of prosecution under the Espionage Act to the protection of whatever defense of "nondefense" information War Department officials might want to protect.

Army Regulations 330–5 were superseded and consolidated with amendments by Army Regulations 380–5 on June 10, 1939, entitled "Safeguarding Military Information." They were subsequently revised and reissued on June 18, 1941.[15]

First Security Classification Executive Order

The first use of an Executive order in the security classification field took place in 1940, when President Roosevelt issued an order entitled "Defining Certain Vital Military and Naval Installations and Equipment." [16] As authority, he cited the act of January 12, 1938 (Public Law 418, 75th Cong., 52 Stat. 3), which stated:

> Whenever, in the interests of national defense, the President defines certain vital military and naval installations or equipment as requiring protection against the general dissemination of information thereto, it shall be unlawful to make any photograph, sketch, picture, drawing, map, or graphical representation of such vital military and naval installation or equipment without first obtaining permission of the commanding officer. * * *

Violation of the law was subject to criminal action, a $1,000 fine and/or imprisonment of up to 1 year.[17]

[14] Ibid., p. 41.
[15] Ibid., p. 37.
[16] Executive Order No. 8381; Federal Register, Mar. 26, 1940, vol. 5, p. 1145 et seq.
[17] Now codified as part of the Espionage Act as 18 U.S.C. 795(a).

In defining the installations or equipment requiring protection, the President listed as a criterion the classification as "Secret," "Confidential," or "Restricted" under the direction of either the Secretary of War or the Secretary of the Navy. In addition to military or naval installations, weapons, and equipment so classified or marked, included in the definition were:[18]

> All official military or naval books, pamphlets, documents, reports, maps, charts, plans, designs, models, drawings, photographs, contracts, or specifications, which are now marked under the authority or at the direction of the Secretary of War or the Secretary of the Navy as "secret," "confidential," or "restricted," and all such articles or equipment which may hereafter be so marked with the approval or at the direction of the President.

In his study of Executive Order 8381 and Public Law 418, Irvine makes these comments on the legislative history of the act, contained in the House debates on S. 1485:[19]

> Congress, in passing the act of January 12, 1938, can hardly have expected that it would be interpreted to be applicable to documentary materials as "equipment." * * * The provisions of the Executive order were probably a substitute for equivalent express provisions of law that Congress could not be expected to enact. Mention may be made in this connection of the refusal of Congress, long after the attack on Pearl Harbor, to pass the proposed War Security Act submitted to Congress by Attorney General Francis Biddle on October 17, 1942 (H.R. 1205, 78th Cong., 1st sess.).

Office of War Information Classification System

A Government-wide regulation dealing with security classification was issued in September 1942, by the Office of War Information under authority vested by Executive Orders 9103 and 9182.[20] This regulation, a forerunner of subsequent classification Executive orders, provided definitions of classified information—"Secret," "Confidential," and "Restricted"—and designated authority to classify. It also contained provisions warning against overclassification and provided instructions for the identification of classified information, for its proper dissemination, and proper handling.

The definitions of the three categories were:

> *Secret Information* is information the disclosure of which might endanger national security, or cause serious injury to the Nation or any governmental activity thereof.
>
> *Confidential Information* is information the disclosure of which although not endangering the national security would impair the effectiveness of governmental activity in the prosecution of the war.

[18] Ibid., par. 3, pp. 1147–1148.
[19] Ibid., pp. 48–49; see also Congressional Record, vol. 83, pt. 1, Jan. 5, 1938, pp. 70–72.
[20] Office of War Information Regulation No. 4, issued Sept. 28, 1942; amended, Nov. 13, 1942. A copy of the regulation is in the files of the Foreign Operations and Government Information Subcommittee.

> *Restricted Information* is information the disclosure of which should be limited for reasons of administrative privacy, or is information not classified as confidential because the benefits to be gained by a lower classification, such as permitting wider dissemination where necessary to effect the expeditious accomplishment of a particular project, outweigh the value of the additional security obtainable from the higher classification.

Supplement No. 1 to OWI Regulation No. 4, issued on May 19, 1943, created the Security Advisory Board (SAB), consisting of Army and Navy officers who were charged with responsibilities as "an advisory and coordinating board in all matters relating to carrying out the provisions of OWI Regulation No. 4." [21]

After the end of World War II, the SAB continued to function as a part of the State-War-Navy Coordinating Committee—later the State-Army-Navy-Air Force Coordinating Committee. On March 21, 1947, provisions of Executive Order 9835 directed the SAB to draft rules for the handling and transmission of documents and information that should not be disclosed to the public. A preliminary draft was completed by the SAB but were not issued before the SAB and its parent coordinating committee went out of existence.[22]

After enactment of the National Security Act in 1947, which created the National Security Council (NSC), the NSC was given responsibility to consider and study security matters, which involve many executive departments and agencies, and to make recommendations to the President in this vital area. The Interdepartmental Committee on Internal Security (ICIS) was subsequently created and the activity of this committee was, according to the Wright Commission report, responsible for issuance of Executive Order 10290 in 1951.[23]

Executive Order 10104 Issued by President Truman

The 1940 Executive Order 8381 was superseded 10 years later by President Truman's Executive Order 10104, "Definitions of Vital Military and Naval Installations and Equipment." [24] The new order continued authorization for the same three classification markings as in the previous order and formalized the designation "Top Secret," which had been added to military regulations during the latter part of World War I to coincide with classification levels of our allies. The order gave the Secretary of Defense and the Secretaries of the Army, Navy, and Air Force the authority to classify or direct to be classified the types of information described in the order.

It is important to emphasize that through the historical period of the use of classification markings described thus far until 1950, such formal directives, regulations, or Executive orders applied to the protection of military secrets, rarely extending into either those affecting nonmilitary agencies or those involving foreign policy or

[21] A copy is in the files of the Foreign Operations and Government Information Subcommittee. A later SAB coordinating committee included representation from the State Department.
[22] Hearings, Subcommittee on Reorganization, Senate Government Operations Committee, 84th Cong., 1st sess. on S.J. Res. 21, to establish a Commission on Government Security; testimony of Assistant Attorney General William F. Tompkins, p. 30.
[23] Report of the Commission on Government Security, supra, p. 155.
[24] Federal Register, vol. 15, p. 597, et seq., Feb. 1, 1950.

diplomatic relations. One exception is in the area of communications secrecy, governed by section 798 of the Espionage Act. This law, which protects cryptographic systems, communications intelligence information, and similar matters, applies, of course, to both military and nonmilitary Federal agencies such as the State Department. Aside from more restrictive war-time regulations, nonmilitary agencies had, until 1958, relied generally on the 1789 "housekeeping" statute mentioned earlier as the basis for withholding vast amounts of information from public disclosure.[25]

Executive Order 10290 Issued by President Truman

On September 24, 1951, President Truman issued a new Executive order formalizing and extending the security classification system within nonmilitary agencies as well as the Defense Establishment. The order, entitled "Prescribing Regulations Establishing Minimum Standards for the Classification, Transmission, and Handling, by Departments and Agencies of the Executive Branch, of Official Information Which Requires Safeguarding in the Interest of the Security of the United States." [26] It permitted any executive department or agency to classify information on a uniform basis and defined "classified security information" to mean "official information the safeguarding of which is necessary in the interest of national security, and which is classified for such purposes by appropriate classifying authority." [27]

The order was strongly criticized by some segments of the press for its vagueness and potential abuses it made possible and also by a number of Members of Congress. A bill (S. 2190) was introduced on September 28, 1951, to "prohibit unreasonable suppression of information by the Executive Branch of the Government," which, in effect, would have repealed the Executive order.[28] No action was taken on the measure.

Executive Order 10501 Issued by President Eisenhower

When President Eisenhower took office in January 1953, he took notice of the widespread criticism of Executive Order 10290 and requested Attorney General Brownell for advice concerning its recision or revision. On June 15, 1953, the Attorney General recommended recision of the Executive order and the issuance of a new order which would "protect every requirement of national safety and, at the same time, honor the basic tenents of freedom of information." [29]

[25] For a discussion of the use of this statute by executive agencies, see H. Rept. 1461, 85th Cong, 2d sess., Mar. 6, 1958, accompanying H.R. 2767, legislation which was subsequently enacted as Public Law 85-619.

[26] Executive Order No. 10290, Federal Register, Sept. 27, 1951, vol. 16. p. 9795 et seq.

[27] Ibid., pt. II, par. 4, p. 9797.

[28] See H. Rept. 2456, 87th Cong., 2d sess. "Safeguarding Official Information in the Interests of the Defense of the United States (The Status of Executive Order 10501)," issued by this committee on Sept. 21, 1962, for background on the controversy over Executive Order 10290; particularly see pp. 27–35 for text of staff memorandum No. 82–1–60 of Senate Committee on Expenditures in the Executive Departments, dated Nov. 29, 1951, on the constitutional and legal aspects of S. 2190. See also Carol M. Barker and Matthew H. Fox, Classified Files: The Yellowing Pages, A Report on Scholar's Access to Government Documents; New York: The Twentieth Century Fund, 1972, pp. 12–13.

[29] Report of the Commission on Government Security, supra, p. 155.

That fall, President Eisenhower replaced the controversial Truman order with Executive Order No. 10501, "Safeguarding Official Information in the Interests of the Defense of the United States." [30] This order, issued on November 5, 1953, became effective on December 15, 1953; it was amended several times in the succeeding years, but for almost 20 years served as the basis for the security classification system until it was superseded in March 1972.

Executive Order No. 10501 reduced the number of agencies authorized to classify such information, eliminated the "restricted" category, and redefined the usage of the three classification markings authorized:

> SECTION 1. *Classification Categories:* Official information which requires protection in the interests of national defense shall be limited to three categories of classification which in descending order of importance shall carry one of the following designations: Top Secret, Secret, or Confidential. No other designation shall be used to classify defense information, including military information, as requiring protection in the interests of national defense, except as expressly provided by statute. These categories are defined as follows:
>
> (a) *Top Secret:* Except as may be expressly provided by statute, the use of the classification Top Secret shall be authorized, by appropriate authority, only for defense information or material which requires the highest degree of protection. The Top Secret classification shall be applied only to that information or material the defense aspect of which is paramount, and the unauthorized disclosure of which could result in exceptionally grave damage to the Nation such as leading to a definite break in diplomatic relations affecting the defense of the United States, an armed attack against the United States or its allies, a war, or the compromise of military or defense plans, or intelligence operations, or scientific or technological developments vital to the national defense.
>
> (b) *Secret:* Except as may be expressly provided by statute, the use of the classification Secret shall be authorized, by appropriate authority, only for defense information or material the unauthorized disclosure of which could result in serious damage to the Nation, such as by jeopardizing the international relations of the United States, endangering the effectiveness of a program or policy of vital importance to the national defense, or compromising important military or defense plans, scientific or technological developments important to national defense, or information revealing important intelligence operations.
>
> (c) *Confidential:* Except as may be expressly provided by statute, the use of the classification Confidential shall be authorized, by appropriate authority, only for defense information or material the unauthorized disclosure of which could be prejudicial to the defense interests of the Nation.

[30] Federal Register, Nov. 9, 1953, vol. 18, p. 7049 et seq.; it was amended by Executive Order No. 10816, May 8, 1959, 24 F.R. 3777; Executive Order No. 10901, Jan. 11, 1961, 26 F.R. 217; Executive Order No. 10964, Sept. 20, 1961, 26 F.R. 8932; Executive Order No. 10985, Jan. 15, 1962, 27 F.R. 439; Executive Order No. 11097, Mar. 6, 1963, 28 F.R. 2225; Executive Order No. 11382, Nov. 28, 1967, 32 F.R. 16247. See also H. Rept. 2456.

Elimination of the "Restricted" category, applied to training manuals and great volumes of documents having limited sensitivity, resulted in the removal of much information previously included within the classification system. The review of massive amounts of such "Restricted" data also resulted in the elevation of some documents to the "Confidential" level.

Legal Authority for Executive Order 10501

Executive Order 10501 contained only a general statement of its legal authority in the preface:

> Now, therefore, by virtue of the authority vested in me by the Constitution and statutes, and as President of the United States, and deeming such action necessary in the best interests of the national security, it is hereby ordered as follows * * *

The President, like his predecessor, was apparently relying primarily on implied constitutional powers of his office and statutes claimed to afford a basis on which to justify the issuance of the Executive order. No specific statutory authority for it was cited. A 1960 study by the American Law Division, Legislative Reference Service, Library of Congress, for this committee's Special Subcommittee on Government Information on the statutory basis supporting the issuance of Executive Order 10501 stated:[31]

> * * * it would seem that if there had been a specific statutory basis for the order, the President would have specifically relied upon it in issuing the order. Further, an extensive search fails to reveal any statute which specifically authorized the President to issue such an order. From the foregoing it must be assumed that the President issued Executive Order 10501 under an implied constitutional power. (See Constitution, art. II, sec. 1, vesting executive power in the President; art. II, sec. 2, providing that the President shall be Commander in Chief of the Armed Forces; and art. II, sec. 3, requiring him to take care that the laws be faithfully executed.) The extent of the President's constitutional power to control the disclosure by persons in the executive branch of the Government and to withhold information from the Congress and the public has long been in controversy and has never been fully settled.

In addition to the broad constitutional authority for the Executive order mentioned earlier, a statement of express legal authority for its issuance was contained in the 1957 Report of the Commission on Government Security (the Wright Commission). It lists as implied statutory authority (1) the 1789 "house-keeping" statute (subsequently curtailed in this respect by the 1958 amendment); (2) sections of the Espionage Act, such as 18 U.S.C. 795(a) and 18 U.S.C. 798; (3) sections of the Internal Security Act of 1950, such as 4(b) and 4(c) (50 U.S.C. 781); and finally, (4) most strongly on authority contained in the National Security Act of 1947, which created the National Security Council (NSC) (50 U.S.C. 401).[32]

[31] H. Rept. 2456, 87th Cong., supra, pp. 36–37.
[32] Report of the Commission on Government Security, supra, p. 158–159.

In 1970, the Senate Foreign Relations Committee's Subcommittee on U.S. Security Agreements and Commitments Abroad conducted extensive hearings which again raised the question of President Eisenhower's authority to issue Executive Order 10501 in 1953. The legal adviser of the State Department, Mr. John R. Stevenson, with the approval of the Justice Department, referred the committee to the above statement contained in the 1957 Report of the Commission on Government Security for the legal basis.[33]

The 1970 State Department memorandum by Mr. Stevenson also cited as legal authority for Executive Order 10501 provisions of (1) the Atomic Energy Act of 1954 (a revision of the Atomic Energy Act of 1946), section 142, which recognizes defense information and intelligence information as part of the definition it gives to "Restricted Data," affecting nuclear weapons and material; (2) provisions of the Foreign Assistance Act of 1961, as amended, such as section 634(b) and 634(c); (3) provisions of the Arms Control and Disarmament Act of 1961, as amended, such as section 45(a) and 45(b); and finally (4) the Freedom of Information Act, exemption 552(b)(1), which permits the withholding of matters "specifically required by Executive order to be kept secret in the interest of national defense or foreign policy." [34]

Automatic Downgrading and Declassification Amendments

Amendments over the years to Executive Order 10501 dealt with relatively minor technical matters, such as the adding of new agencies to those already possessing classification authority or the deletion of agencies from the list.[35] The most significant amendment was contained in Executive Order 10964, issued by President Kennedy on September 20, 1961, which set up an automatic declassification and downgrading system. It established four groups of categories of information to be subject to such "automatic changes": [36]

> (a) *Automatic Changes:* In order to insure uniform procedures for automatic changes, heads of departments and agencies having authority for original classification of information or material, as set forth in section 2, shall categorize such classified information or material into the following groups:
>
> (1) *Group 1:* Information or material originated by foreign governments or international organizations and over which the United States Government has no jurisdiction, information or material provided for by statutes such as the Atomic Energy Act, and information or material requiring special handling, such as intelligence and cryptography. This information and material is excluded from automatic downgrading or declassification.

[33] U.S. Congress, Senate Committee on Foreign Relations, Subcommittee on U.S. Security Agreements and Commitments Abroad, 91st Cong., hearings, vol. II, pp. 2008-2011; see also committee print, Senate Foreign Relations Committee, "Security Classification as a Problem in the Congressional Role in Foreign Policy," prepared by the Foreign Affairs Division, Legislative Reference Service, Library of Congress, Dec. 1971, pp. 5-13.

[34] Senate Foreign Relations Committee, committee print, December 1971, supra., pp. 10-13.

[35] Ibid., see pp. 11-12 for chronology of amendments and brief description of each.

[36] Federal Register, Sept. 20, 1961, vol. 26, p. 8932, et seq. The quoted portion is taken from sec. 4(a) of Executive Order 10501, as amended.

(2) *Group 2:* Extremely sensitive information or material which the head of the agency or his designees exempt, on an individual basis, from automatic downgrading and declassification.

(3) *Group 3:* Information or material which warrants some degree of classification for an indefinite period. Such information or material shall become automatically downgraded at 12-year intervals until the lowest classification is reached, but shall not become automatically declassified.

(4) *Group 4:* Information or material which does not qualify for, or is not assigned to, one of the first three groups. Such information or material shall become automatically downgraded at three-year intervals until the lowest classification is reached, and shall be automatically declassified twelve years after date of issuance.

The 1961 amendment also required that, "to the fullest extent practicable" classification authorities "indicate on the information or material at the time of original classification if it can be downgraded or declassified at an earlier date, or if it can be downgraded or declassified after a specific event, or upon the removal of classified attachments or enclosures." Authorization to so mark existing classified information for automatic downgrading and declassification was also provided in the order, although it was not required that they do so.

Summary

The security pendulum thus swung from one extreme to the other during the period of slightly over a decade—from pre-World War II through the immediate post-World War II "Cold War" and through the Korean war years. Efforts to impose a stringent security classification system by President Truman in the early "Cold War" years contrasted sharply with what has been described as "the rather cavalier attitude prevailing before World War II, when secrecy restrictions in the State Department and the Military Establishment were by and large erratic and lax." [37]

Among events that may have affected this trend that followed the stringent war-time security measures of World War II were the aggressive post-war policies pursued by the Soviet Union—their takeover of Eastern European governments; the Berlin Blockade; their development of atomic and hydrogen weapons; and Communist attempts to win political control of Western European countries such as Italy and France. Such actions, in turn, resulted in U.S. responses—the Marshall plan of economic and military assistance to friendly threatened nations; the establishment of the National Security Council (NSC) and the Central Intelligence Agency (CIA); and the creation of the North Atlantic Treaty Organization (NATO) and other similar global defense alliances.

At the same time vast changes were taking place in Asia—the rise of Communist forces in China, the ensuing civil war and expulsion of the nationalist government from the mainland; the outbreak of hostilities in Southeast Asia between Communist and non-Communist forces and European colonial empires; and the festering struggle between Communist and non-Communist governments that erupted in the Korean war.

[37] Classified files, op. cit., pp. 11–12.

In the United States there was an increasing preoccupation with alleged domestic subversion, highlighted by "spy trials," the enactment of the Internal Security Act of 1950 over President Truman's veto, and culminating in the widespread "loyalty-security" alarm associated with the late Senator Joseph R. McCarthy's extreme accusations against the State and Defense Departments and other sensitive Government agencies.

The trend toward more restrictive policies by executive agencies in their disclosure of information falling into the defense and foreign policy areas during the late 1940's and early 1950's was perhaps a reflection of the vast changes taking place in connection with the growing U.S. role as global leader of the free world.

III. PREVIOUS STUDIES OF SECURITY CLASSIFICATION SYSTEM

In July 1956, the Special Government Information Subcommittee of the House Government Operations Committee began a series of hearings on information problems in the Department of Defense (DOD). The subcommittee, established in June 1955, was headed by Representative John E. Moss of California. These hearings were part of a review of the availability of information from Federal executive agencies.

The Coolidge Committee

A month after the hearings began, then Secretary of Defense Charles E. Wilson, named a 5-member Committee on Classified Information and appointed as its chairman, Mr. Charles A. Coolidge, a prominent Boston lawyer and former Assistant Secretary of Defense. The Committee was thereafter known as the Coolidge Committee.[38]

In his August 13, 1956, letter establishing the Committee, Wilson described to Coolidge its broad purpose:

> As you are aware, I am seriously concerned over the unauthorized disclosure of classified military information. I am, therefore, forming a committee to study the problem and suggest methods and procedures to eliminate this threat to the national security.

The broad mandate given to the Coolidge Committee included "a review of present laws, Executive orders, Department of Defense regulations and directives pertaining to the classification of information and the safeguarding of classified information, to evaluate the adequacy and effectiveness of such documents." [39] Also to be examined were "organizations procedures" in such areas as fixing the responsibility for unauthorized disclosure of classified information, the adequacy of measures to protect against such unauthorized disclosure, and the adequacy of existing laws and other internal regulations in the field of security classification.

The Pentagon "leaks" of classified information appearing in the press earlier that year revealed sharp disagreements among the military services over their respective roles and missions in the atomic-missile era which triggered the creation of the Coolidge Committee.

[38] For full background on the DOD information policy investigation by the subcommittee, see hearings, "Availability of Information From Federal Departments and Agencies," 17 parts, 84th and 85th Cong. (1956–1957); see also H. Rept. 2947 (84th Cong.), H. Rept. 1619, H. Rept. 1884, and H. Rept. 2578 (85th Cong.); a full report on the work of the Coolidge Committee is contained in H. Rept. 1884, June 16, 1958, pp. 20–37. Other members of the Committee were four senior retired military officers: Adm. William M. Fechtler, U.S.N. (retired), Gen. John E. Hull, U.S.A. (retired), Gen. Gerald C. Thomas, U.S.M.C. (retired), and Lt. Gen. Idwal H. Edwards, U.S.A.F. (retired).

[39] Hearings, op. cit., pt. 8, p. 2010.

The "final straw" was apparently a story in the July 12, 1956, New York Times which stated that the Joint Chiefs of Staff were studying a proposal to reduce the Nation's Armed Forces by 800,000 men by the year 1960.[40]

The instructions to the Coolidge Committee made no mention of studying overclassification or arbitrary withholding of information from the public and from Congress. In a September 25, 1956, letter to Secretary Wilson, Chairman Moss of the Special Government Information Subcommittee expressed the hope that the Coolidge Committee would also review the withholding aspects of the problem, as had been revealed in the earlier subcommittee hearings. He was assured in an October 9, 1956, response from Assistant Secretary of Defense Ross that since the two subjects are related "it is probable that the report of the Coolidge Committee will make recommendations bearing on our public information policies as well as our procedures for preventing the unauthorized disclosure of classified military information." [41]

After a 3-month study, the Coolidge Committee concluded in its report of November 8, 1956: [42]

> * * * The two major shortcomings in the operation of the classification system are overclassification and deliberate unauthorized disclosures. We further conclude that little, if any, progress can be made without a successful attack on these major shortcomings.

The report said that it had found "a tendency on the part of Pentagon officials to 'play it safe' and overclassify; an abuse of security to classify administrative matters; attempts to classify the unclassifiable; confusion from basing security on shifting foreign policy; and a failure to declassify material which no longer requires a secrecy label."

The Coolidge Committee informed Secretary Wilson that unnecessary and improper secrecy had reached such "serious proportions" that it was undermining confidence in the entire security system and leading to the very "leaks" that Secretary Wilson sought to prevent. The report stated:

> For all these reasons overclassification has reached serious proportions. The result is not only that the system fails to supply to the public information which its proper operation would supply, but the system has become so overloaded that proper protection of information which should be protected has suffered. The press regards the stamp of classification with feelings which vary from indifference to active contempt. Within the Department of Defense itself the mass of classified papers has inevitably resulted in a casual attitude toward classified information, at least on the part of many.

In its recommendations, the Coolidge Committee made a number of suggestions for plugging "leaks" of classified information, although some were characterized by the Government Information Subcommittee as being "repressive and restrictive." [43] In addition, the Coolidge

[40] H. Rept. 1884, 85th Cong., pp. 20-21; p. 27.
[41] Ibid., p. 22.
[42] Ibid., pp. 23-24; pp. 97-99.
[43] Ibid., pp. 24-31; also pp. 10-14, pp. 60-68, pp. 97-125; Mr. Coolidge testified on the report of his committee on Mar. 11 and 12, 1957; see hearings, op. cit., pt. 8, p. 2011 et seq.

group made some constructive recommendations for eliminating unnecessary secrecy. Among these were recommendations for a "declassification director;" a halt to secrecy changes based on temporary shifts in foreign policy; an explanation to the press when information is refused because it is classified; a determined attack on overclassification; a halt to attempts to classify the unclassifiable; a prohibition on the use of secrecy classification for administrative matters; and improved procedures for releasing information about differences of opinion between the services.

Secretary Wilson issued a new DOD directive covering the procedures for classification of security information under Executive Order 10501. His July 8, 1957, action replaced a dozen previous directives and memorandums and consolidated classification instructions into a single new document—DOD Directive 5200.1—entitled "Safeguarding Official Information in the Interests of the Defense of the United States." [44] It incorporated a number of the specific recommendations made by the Coolidge Committee.

Despite concern over the problem of overclassification, the Coolidge Committee made no recommendation for penalties or disciplinary action in cases of misuse or abuse of classification.[45] The new DOD directive did mention disciplinary action for overclassification, but there is no evidence of its ever having been used.

Vice Adm. John N. Hoskins was appointed as Director of Declassification Policy and subsequently testified before the Government Information Subcommittee on November 18, 1957: [46]

> * * * when you overclassify, you weaken the whole security system. * * * Throughout the 180 years of our Government, however, I have never known a man to be court-martialed for overclassifying a paper, and that is the reason, I am afraid, we are in the mess we are in today. * * *

The Wright Commission

Paralleling the work of the Coolidge Committee was that of another group with Government-wide scope, the Commission on Government Security, established in 1955 by Public Law 304, 84th Congress. The Commission became known as the Wright Commission, named for its chairman, Mr. Loyd Wright, a Los Angeles attorney and former president of the American Bar Association. The 12-member Commission was composed of six Republicans and six Democrats; four members were appointed by the President, four by the Speaker of the House, and four by the President of the Senate.

Its mandate was set forth in section 6 of the law:

[44] Ibid., pp. 107–116; see also hearings, supra., pt. 13, pp. 3239–3271 for the text of DOD Secretary Wilson's memorandum implementing recommendations of Coolidge Committee; see hearings, "U.S. Government Information Policies and Practices—The Pentagon Papers," pt. 2, Foreign Operations and Government Information Subcommittee, June 28 and 29, 1971, pp. 558–597 for amended version of DOD Directive 5200.1 (July 10, 1968).

[45] H. Rept. 1884, 85th Cong., 2d sess., "Availability of Information From Federal Departments and Agencies," pp. 105–106; p. 109.

[46] Hearings, "Availability of Information From Federal Departments and Agencies", op. cit., pt. 13, p. 3055.

> SEC. 6. The Commission [on Government Security] shall study and investigate the entire Government Security Program, including the various statutes, Presidential orders, and administrative regulations and directives under which the Government seeks to protect the national security, national defense secrets, and public and private defense installations, against loss or injury arising from espionage, disloyalty, subversive activity, sabotage, or unauthorized disclosures, together with the actual manner in which such statutes, Presidential orders, administrative regulations, and directives have been and are being administered and implemented, with a view to determining whether existing requirements, practices, and procedures are in accordance with the policies set forth in the first section of this joint resolution, and to recommending such changes as it may determine are necessary or desirable. The Commission shall also consider and submit reports and recommendations on the adequacy or deficiencies of existing statutes, Presidential orders, administrative regulations, and directives, and the administration of such statutes, orders, regulations, and directives, from the standpoints of internal consistency of the overall security program and effective protection and maintenance of the national security.

The Commission organized in December 1955, and was sworn in on January 9, 1956. It employed a supervisory staff, which soon began the task of gathering and analyzing relevant material obtained from executive departments, agencies, and other sources. The Commission held no public hearings, made no statements describing its activities, but conducted extensive interviews with persons throughout the country, both in and out of the Federal Government, who had knowledge and experience in the field. Much additional information was obtained from congressional hearings, studies, and reports.[47]

The Wright Commission issued its 807-page report on June 23, 1957. It covered a dozen related subject areas and made numerous findings and recommendations in such fields as: (1) the Federal civilian loyalty program; (2) military personnel program; (3) document classification program; (4) atomic energy program; (5) industrial security program; (6) port security program; (7) internal organizations program; (8) passport security program; (9) civil air transport security program; (10) immigration and nationality program; (11) criminal statutes; (12) special studies; and finally, the Commission's proposed legislation and Executive orders.[48]

Of particular relevance to the subject of this report is the section of the Wright Commission's report on document classification.[49] The Commission said that it made detailed inquiries of 15 executive departments and agencies concerned with this problem and that it had also studied hearings and other studies of the House Government Information Subcommittee. In its report, the Commission also traced

[47] Report of the Commission on Government Security, op. cit., foreword, pp. xiii-xvi.
[48] Ibid., see pp. xvii-xxiii for summary of recommendations.
[49] Ibid., pp. 151-184.

the history of document classification, which it called "a form of combined censorship and information restriction": [50]

> The advent of World War I brought the first organized approach to document classification as a means of general restriction on public access to information. Censorship policies for control of published information commenced on March 24, 1917, with the promulgation of regulations by the State, War, and Navy Departments. Newspapers were asked to adhere voluntarily. One of the regulations requested that "no information, reports, or rumors, attributing a policy to the government in any international situation, not authorized by the President or a member of the Cabinet, be published without first consulting the Department of State." [51]
>
> On April 13, 1917, by Executive Order 2594, President Wilson created the Committee on Public Information, named George Creel as chairman, and World War I censorship formally got under way. Creel thought that censorship as practiced at that time was unworkable. He described the whole effort as of a piece with "the hysterical shush-shushing that warned against unguarded speech, just as though every citizen possessed some important military secret." He said, at the end of the War, that "virtually everything we asked the press not to print was seen or known by thousands." Creel believed the answer to be "secrecy at the source" through action by the military departments without depending upon press judgment.

According to the Wright Commission report, "a much more efficient and effective system of information control" was employed during World War II, that "profited by the mistakes of World War I." In describing the World War II system the report said: [52]

> It separated propaganda and censorship and, in effect, supported by voluntary agreement the withholding of information which the Armed Forces thought dangerous to disclose. It was, in reality, a system for making effective the theory of censorship at the sources of information that Creel had talked about at the end of World War I.
>
> The first formal effort to withhold information in World War II came on December 31, 1940, when Secretary of Navy Frank Knox asked radio, news, and picture editors to avoid any mention of: (1) Actual or intended movements of vessels or aircraft of the United States Navy, units of naval enlistment personnel or divisions of mobilized reserves, or troop movements of the United States Marine Corps; (2) New United States Navy ships or aircraft; (3) United States Navy construction projects ashore.

---

[50] Ibid., p. 153.
[51] Ibid., quoting James Russell Wiggins, Freedom or Secrecy, Oxford University Press: New York, 1956, pp. 95–96.
[52] Ibid., pp. 153–154.

During 1941 as America stepped up defense production and planning, information control tightened up. In September, the War and Navy Departments disclosed they were making plans for censorship of all outgoing communications. When the United States declared war, on December 8, J. Edgar Hoover was made temporary coordinator of all news and communications censorship. The President at this time appealed to press and radio to refrain from the publication of unconfirmed reports. Various Federal agencies took steps to curtail their information. The Weather Bureau, for example, began to restrict its reports.

When the first code of wartime practices for newspapers, magazines, and other periodicals was issued on January 15, 1942, wartime censorship was formally launched. The code was revised each 6 months thereafter. It described categories of news that were not to be published without appropriate authority, listing in 17 different clauses the information that required authorization before publication. The significant words in the operation of this wartime information code were "appropriate authority." The Office of Censorship did not undertake to suppress information that "appropriate authority" officially gave out. The Office of Censorship was terminated by Executive Order 9631, effective November 15, 1945.

The Office of War Information (OWI) was established within the Office for Emergency Management by Executive Order 9182 of June 13, 1942. The OWI consolidated into one agency all foreign and domestic war information functions of the Government. Its purpose was to "provide an intelligent understanding of the status and progress of the war effort policies, activities and aims of the Government." [53] The OWI regulation relating its activities to the classification system is discussed at pages 7–8 of this report.

The Wright Commission also reviewed the operation of Executive Order 10501, issued a few years earlier by President Eisenhower. It found that some 1.5 million employees of Federal departments and agencies had the authority to classify documents as of January 1, 1957.[54] The Wright Commission recommended that the "Confidential" category of information under Executive Order 10501 be eliminated, criticizing the overuse of this label and its restriction upon the free exchange of information in the scientific and technological areas which retards progress necessary to our national security. It estimated that 59 percent of all Defense Department classified information was "Confidential," while 76 percent of classified information in the State and Commerce Departments was similarly marked. It also recommended that the numbers of persons in each agency authorized to classify documents under Executive Order 10501 be reduced. It also recommended that document classification training programs be instituted. Another recommendation urged the creation of a statutory Central Security Office having "review and advisory functions with respect to the Federal document classification program and to make recommendations for its improvement as needed."

[53] Ibid., p. 154.
[54] Ibid., p. 177.

The most controversial portion of the Wright Commission recommendations was its proposal urging Congress to "enact legislation making it a crime for any person willfully to disclose without proper authorization, for any purpose whatever, information classified 'secret' or 'top secret,' knowing, or having reasonable grounds to believe, such information to have been so classified." [55] The recommended bill would impose a $10,000 fine and jail term of up to 5 years for those convicted of violating its provisions. The Commission made it clear that its proposal was aimed at persons outside of government, such as newsmen. The recommendation was soundly criticized in articles and editorials from such papers as the New York Times, Baltimore Sun, Chicago Daily Sun-Times, Boston Traveler, Cleveland Plain Dealer, Detroit Free Press, Washington Post and Times Herald, and Editor and Publisher. One article by James Reston of the New York Times pointed out that it would have even resulted in the prosecution of the reporter, Paul Anderson of the St. Louis Post-Dispatch, who uncovered and published "secret" documents in the "Teapot Dome" scandal during the 1920's.

Subsequent correspondence between Subcommittee Chairman Moss and Commission Chairman Wright sought to obtain specific examples of instances where the Commission could document the "purloining" of classified documents by the press. However, Chairman Wright provided no specific names and in subsequent testimony before the subcommittee by Pentagon officials denied knowledge about any specific instances of the purloining of classified documents.[56]

House Government Information Subcommittee Studies

In its 2-year study of security classification policies that spanned the Coolidge and Wright groups, the House Government Information Subcommittee concentrated heavily on the Department of Defense. The conclusions and recommendations made, in turn, through reports of the full Government Operations Committee are particularly important to recall because they pinpointed major problem areas which existed over 15 years ago. They also proposed a number of specific recommendations to correct many of these problems (see pp. 23–27 of this report)—recommendations that were largely ignored by both Republican and Democratic administrations. Had such recommendations been properly implemented by top Pentagon officials, it is possible that the security classification "mess" referred to by President Nixon almost 14 years after the issuance of the first of these committee reports could have long since been corrected. Many of the committee's conclusions could have been written today, instead of in 1958. For example, in discussing the handling of information by the Military Establishment, the committee concluded: [57]

> Never before in our democratic form of government has the need for candor been so great. The Nation can no longer afford the danger of withholding information merely because the facts fail to fit a predetermined "policy." Withholding

[55] H. Rept. 1884, op. cit., pp. 14–19; pp. 31–39.
[56] Ibid., see also hearings, op. cit., pt. 13, pp. 3304–3305 (text of proposed bill) and pp. 3305–3320 for correspondence and material related to this controversy.
[57] H. Rept. 1884 (85th Cong., 2d sess.), "Availability of Information From Federal Departments and Agencies (Department of Defense)," June 16, 1958, p. 152.

> for any reason other than true military security inevitably results in the loss of public confidence—or a greater tragedy. Unfortunately, in no other part of our Government has it been so easy to substitute secrecy for candor and to equate suppression with security.
>
> * * * In a conflict between the right to know and the need to protect true military secrets from a potential enemy, there can be no valid argument against secrecy. The right to know has suffered, however, in the confusion over the demarcation between secrecy for true security reasons and secrecy for "policy" reasons. The proper imposition of secrecy in some situations is a matter of judgment. Although an official faces disciplinary action for the failure to classify information which should be secret, no instance has been found of an official being disciplined for classifying material which should have been made public. The tendency to "play it safe" and use the secrecy stamp, has, therefore, been virtually inevitable.
>
> Abuse of the security classifications under Executive Order 10501 has been only one part of the unnecessary secrecy in violation of the right to know. Equally important—although entirely distinct—have been restrictions on information about the day-to-day operations of government, ineligible by any stretch of the imagination for secrecy labels on grounds of military security.

After discussing the charges by Chairman Loyd Wright of the Commission on Government Security about the alleged "purloining" of classified documents by newsmen, the committee concluded: [68]

> Mr. Wright's indictment of the press is symptomatic of self-styled security experts who point an accusing finger at newsmen for stories which often are based on properly cleared or otherwise publicly available information. The trail which Mr. Wright seeks to blaze in the wilderness of excessive secrecy leads inevitably to censorship unparalleled in this country, even in time of war.
>
> No member of the press should be immune from responsibility if sound evidence can be produced to prove that he has in fact deliberately "purloined" and knowingly breached proper classified military secrets. But the press must not be made the whipping boy for weaknesses in the security system caused by overzealous censors who misuse that system to hide controversy and embarrassment.

The committee also concluded: [69]

> Capricious censorship by the Office of the Assistant Secretary of Defense (Public Affairs) has been a major factor in undermining the Military Establishment's security system. As long as arbitrary restrictions for reasons of "policy" are intermingled without distinction with restrictions for true security, it is impossible to expect military and civilian personnel, the press, the public or the Congress to have respect for the security labels authorized under Executive Order 10501.

[68] Ibid., pp. 154–155.
[69] Ibid., pp. 155–158.

> * * * Despite some improvements, the Defense Department's security classification still is geared to a policy under which an official faces stern punishment for failure to use a secrecy stamp but faces no such punishment for abusing the privilege of secrecy, even to hide controversy, error, or dishonesty.

Earlier Recommendations to Improve the Security Classification System

The committee made a number of important recommendations in that report to strengthen the functioning of the security classification system. Among these recommendations were the following:[60]

1. The President should make effective the classification appeals procedure under section 16 of Executive Order 10501 and provide for a realistic, independent appraisal of complaints against overclassification and unjustified withholding of information.
2. The President should make *mandatory* the marking of each classified document with the future date or event after which it will be reviewed or automatically downgraded or declassified.
3. The Secretary of Defense should set a reasonable date for the declassification of the huge backlog of classified information, with a minimum of exceptions.
4. The Secretary of Defense should direct that disciplinary action be taken in cases of overclassification.
5. The Secretary of Defense should completely divorce from the Office of Security Review the function of censorship for *policy* reasons and should require that all changes made or suggested in speeches, articles and other informational material be in writing and state clearly whether the changes are for security or policy reasons.
6. The Secretary of Defense should establish more adequate procedures for airing differences of opinion among responsible leaders of the military services *before* a final policy decision is made.
7. The Congress should reaffirm and strengthen provisions in the National Security Act giving positive assurance to the Secretaries and the military leaders of the services that they will not be penalized in any way if, on their own initiative, they inform the Congress of differences of opinion *after* a policy decision has been made.

As part of its continuing oversight of the operation of the security classification system, the Government Information Subcommittee also pointed out that the provision of Executive Order 10501 ordering that "wherever practicable classified documents bear a date or event for subsequent declassification is being almost totally ignored." [61]

[60] Ibid., p. 161.
[61] H. Rept. 2947 (84th Cong., 2d sess.), p. 89.

Mr. Charles A. Coolidge, Chairman of the Coolidge Committee, testified that 6 billion documents were classified during World War II and that the rate of classification had increased since then.[62] A clear lack of progress in providing for systematic declassification procedures by the Defense Department was noted by the Committee. Vice Admiral Hoskins, Director of the new Office of Declassification Policy, told the subcommittee in November 1957, that a new automatic declassification directive would "soon" be issued by DOD. But this committee noted in H. Rept. 1884 (85th Cong., 2d sess.) on June 16, 1958, that the new directive still had not been issued. Prodding efforts by the subcommittee continued during the summer of 1958.[63]

Finally, on October 3, 1958, the Department of Defense announced the signing of the new declassification directive, DOD Directive 5200.9, dated September 27, 1958. The Department's press release announcing the new directive stated:[64]

> * * * It establishes a new method by which millions of military documents, originated prior to January 1, 1946, and classified top secret, secret, and confidential will now be downgraded or declassified. The new directive which becomes effective 60 days after signature, automatically cancels, except within a few limited categories, the security classifications on millions of documents which no longer need protection in the national interest. In addition, the directive will downgrade to secret all top secret documents which are exempted from declassification. * * *

Unfortunately, this optimistic view of downgrading and declassification progress was not borne out by subsequent events. A report prepared by the Office of Declassification Policy and submitted to the subcommittee on April 15, 1959, outlined a number of positive administrative actions designed to implement the new directive.[65] The Department of Defense estimated that there were 325,000 cubic feet of classified Defense documents which originated prior to 1946.[66]

Additional efforts were made by the subcommittee to reduce the number of executive agencies authorized to exercise classification authority under Executive Order 10501. Studies on the use of classification authority by a list of agencies surveyed by the subcommittee were made available to the White House and on March 9, 1960, President Eisenhower signed a memorandum having the effect of prohibiting some 33 Federal agencies from classifying information under the Executive order.[67] President Eisenhower later issued Executive Order

[62] Hearings, "Availability of Information From Federal Departments and Agencies," pt. 8, p. 2025, Mar. 11, 1957. It should be noted that there are significant differences in assessing problems and costs of declassifying the huge backlog of documents and those of dealing with declassification and downgrading of current classified material as part of an ongoing system.

[63] H. Rept. 2578, 85th Cong., 2d sess., "Availability of Information From Federal Departments and Agencies, Progress of Study—February 1957–July 1958," Aug. 13, 1958, pp. 58–60.

[64] H. Rept. 1137 (86th Cong., 1st sess.), "Availability of Information From Federal Departments and Agencies," (Progress of Study, August 1958–July 1959), Sept. 3, 1959, pp. 81–82; see pp. 87–91 for text of directive.

[65] Ibid., pp. 93–97. An organizational chart of the Hoskins Office appears at p. 98.

[66] Ibid., p. 81. A cubic foot of documents consists of about 2,000 sheets of paper and weighs about 30 pounds. While some progress in cutting into the backlog of World War II documents was made as a result of these policies, it is clear that the objectives of the Hoskins Office fell far short of realization. Fourteen years later President Nixon, in his statement upon issuance of Executive Order 11652, estimated that there were still 160 million pages of World War II classified documents.

[67] H. Rept. 2084 (86th Cong., 2d sess.), "Availability of Information From Federal Departments and Agencies," (The First Five Years and Progress of Study, August 1959–July 1960), July 2, 1960, pp. 164–176.

10901 on January 9, 1961, prohibiting 30 additional agencies from classifying military information, thus limiting classification authority to 45 specifically named departments and agencies.[68]

Still another major improvement in the classification system, advocated by the committee over these years, was the issuance of DOD Directive 5200.10, issued on June 29, 1960. It was also originated by the Hoskins Office. The new directive was originally scheduled to take effect on December 27, 1960, but its effective date was postponed until May 1, 1961.[69] It applied to documents originated on or after January 1, 1946, and established two "time ladders" for automatically downgrading or declassifying documents after specific time levels have elapsed. Nonexempted material would be downgraded at 3-year intervals from top secret to secret to confidential, and automatically declassified after a total of 12 years' existence in a classified status. Exempted material, such as war plans, intelligence documents, and similar information, would be downgraded from top secret to secret to confidential at 12-year intervals, but would not be automatically declassified. The automatic downgrading and declassification provisions of DOD Directive 5200.10 were subsequently incorporated into Executive Order 10964, issued by President Kennedy on September 20, 1961.[70]

Executive Order 10964 also added a new section 19 to Executive Order 10501 directing department heads to "take prompt and stringent administrative action" against Government personnel who knowingly and improperly release classified information. Where appropriate, it directed that such cases be referred to the Justice Department for possible prosecution under applicable criminal statutes.[71]

In its September 22, 1961, report the committee urged President Kennedy to implement previous recommendations to help solve overclassification and other information problems. They were contained in a letter dated February 23, 1961, from Subcommittee Chairman Moss to the President.[72] Among the major recommendations was a proposal to make effective the classification appeals procedure available under section 16 of Executive Order 10501, so as to provide for a realistic independent appraisal of complaints against overclassification and unjustified withholding of information. While the President did designate Mr. Lee C. White, Assistant Special Counsel to the President, as the designated person to receive complaints under section 16, there is no indication that the procedure was utilized.[73]

Subcommittee Chairman Moss also apprised incoming Defense Secretary Robert S. McNamara of previous recommendations in the security classification and public information problem areas in letters dated February 7, March 7, and June 6, 1961.[74] Among the major

[68] H. Rept. 818 (87th Cong., 1st sess.), "Availability of Information From Federal Departments and Agencies," (Progress of Study, July–December 1960), July 28, 1961, pp. 139–154; the text of Executive Order 10901 is at pp. 140–142.
[69] Ibid., pp. 17–39; the text of DOD Directive 5200.10 is at pp. 18–24.
[70] H. Rept. 2456, "Safeguarding Official Information in the Interests of the Defense of the United States (The Status of Executive Order 10501)," (87th Cong. 2d sess.), Sept. 21, 1962, p. 3.
[71] Ibid., p. 5.
[72] H. Rept. 1257, "Availability of Information From Federal Departments and Agencies" (Progress of Study, January-August, 1961), (87th Cong., 1st sess.), Sept. 22, 1961, pp. 153-154. A memorandum listing information problems uncovered by the subcommittee is at pp. 155–165.
[73] H. Rept. 2456, op cit., pp. 7–9. White testified before the subcommittee concerning his White House responsibilities during the 1971 hearings. Hearings, op. cit., pt. 1, pp. 45–91.
[74] H. Rept. 1257, op. cit., pp. 49–59.

recommendations called to Secretary McNamara's attention was one urging that "The Secretary of Defense should direct that disciplinary action be taken in cases of overclassification," which had been made in H. Rept. 1884 in 1958. On May 31, 1961, Secretary McNamara issued DOD Directive 5230–13, setting forth four basic principles of public information policy at the Defense Department, among which was the following.[75]

> Secondly, it is essential to avoid disclosure of information that can be of material assistance to our potential enemies, and thereby weaken our defense position. It is equally important to avoid overclassification, and therefore, I suggest that we follow this principle: When in doubt, underclassify. In no event should overclassification be used to avoid public discussion of controversial matters.* * *

Unfortunately, this "underclassification" principle and the warning against overclassification was not implemented by the imposition of penalties against overclassification, as had been recommended by the committee.

The committee renewed its recommendations in these two major areas involving the more effective operation of the security classification system in its 1962 report on the status of Executive Order 10501:[76]

> But two of the most important security problems which the committee has discussed over the years still remain to be solved. There are strict penalties for failure to protect a document which may have an effect upon the Nation's security, but there are no penalties for those secrecy minded Government officials who abuse the classification system by withholding, in the name of security, all sorts of administrative documents. A security system which carries no penalties for using secrecy stamps to hide errors in judgment, waste, inefficiency, or worse, is perversion of true security. The praiseworthy slogan of Defense Secretary McNamara—"when in doubt, underclassify"—has little effect when there is absolutely no penalty to prevent secrecy from being used to insure individual job security rather than national military security.
>
> The committee strongly urges, therefore, that the Defense Department establish administrative penalties for misuse of the security system, for until the generalizations about the public's right to know are backed up by specific rules and regulations—until set penalties are established for abuse of the classification system—fine promises and friendly phrases cannot dispel the fear that information which has no effect on the Nation's security is being hidden by secrecy stamps.

The other problem, which seems to be no nearer solution today than when it was first posed by the committee (H. Rept. 1884, 85th Cong., p. 161), is the lack of an effective

[75] Ibid., p. 57.
[76] H. Rept. 2456, op. cit., p. 13.

procedure for appeals against abuse of the information classification system. President Kennedy assigned the appeals job to his Assistant Special Counsel, but the incidental assignment to a busy assistant of responsibility for the appeals procedure along with his many other duties does not fill the need for an effective system to handle public appeals against secrecy abuses.

> The committee strongly urges, therefore, that the appeals section of Executive Order 10501 be adequately implemented in an effective manner, for until a responsible individual in the White House is charged with the primary duty of receiving and acting upon complaints against abuse of the classification system—until a fully operating appeals system is set up and widely publicized—the most important safety valve in the information security system is completely useless.

IV. SECURITY CLASSIFICATION AND THE FREEDOM OF INFORMATION ACT

Statutory recognition of the authority of the executive branch to withhold certain classified information from the public was contained in exemption (1) of the Freedom of Information Act:[77]

> (b) This section does not apply to matters that are—
>
> (1) specifically required by Executive order to be kept secret in the interest of national defense or foreign policy; * * *

The legislative history of the act (S. 1160—H.R. 5012) is sketchy with respect to this exemption. Language in the House report relates the provision in exemption (b)(1) to abuses in the withholding of information "in the public interest" under the Administrative Procedure Act:[78]

> * * * The language (of the exemption) both limits the present vague phrase "in the public interest" and gives the area of necessary secrecy a more precise definition. The permission to withhold Government records "in the public interest" is undefinable. In fact, the Department of Justice left it up to each agency to determine what would be withheld under the blanket term "public interest." No Government employee at any level believes that the "public interest" would be served by disclosure of his failures or wrongdoings, but citizens both in and out of Government can agree to restrictions on categories of information which the President has determined must be kept secret to protect the national defense or to advance foreign policy, such as matters classified pursuant to Executive Order 10501.

The 1967 Attorney General's memorandum, providing guidelines to executive departments and agencies in the implementation of the Freedom of Information Act stated:[79]

> To the extent that agencies determine that matters within their responsibility must be kept secret in the interest of the national defense or foreign policy, and are not required to be withheld by Executive order or other authority, they should seek appropriate exemption by Executive order, to come within the language of subsection (e)(1). The reference in the House report to Executive Order 10501 indicates that no great degree of specificity is contemplated in identifying matters subject to this exemption. However, in the interest of providing for the public as much information as possible, an

[77] Sec. 552(b)(1) of title 5, United States Code.
[78] H. Rept. 1497 (89th Cong., 2d sess.), "Clarifying and Protecting the Right of the Public to Information," May 9, 1966, pp. 9–10.
[79] Attorney General's memorandum on the "Public Information Section of the Administrative Procedure Act," U.S. Department of Justice, June 1967, p. 30.

Executive order prepared for the signature of the President in this area should define as precisely as is feasible the categories of matters to be exempted.

Exemption (b)(1) Cases and the Courts

As has been noted in an earlier report on the administration of the FOI Act, the courts have been "generally reluctant to order the disclosure of Government information falling within exemption (b)(1) of the act—information 'specifically required by Executive order to be kept secret in the interest of the national defense or foreign policy.' " [80] Relatively few requests for records involving such information have been made during the 5-year period of executive decisions under the act surveyed by the Foreign Operations and Government Information Subcommittee and at least three such cases have been decided in the courts.[81]

The first instance in which exemption (b)(1) was subject to court review was the 1967 case of *Epstein* v. *Resor*.[82] Prof. Julius Epstein, an historian at Stanford University's Hoover Institution on Revolution, War and Peace, requested a file from the Army under the FOI Act described as "Forcible Repatriation of Displaced Soviet Citizens—Operation Keelhaul," which was classified as top secret since 1948 under a joint agreement between the United States and British Governments. The file contains both American and British documents dealing with the forced repatriation of anti-Communist Russian prisoners of war in the post-World War II period.

When the Army refused to declassify the documents and make them available to Epstein, he sued Secretary of the Army Resor under the FOI Act to enjoin him from withholding the "Operation Keelhaul" file. Epstein asked the court to examine the file of documents in camera to determine whether or not they were properly classified under Executive Order 10501 and if the denial under exemption (b)(1) of the FOI Act was valid.

Both the U.S. District Court and the Ninth Circuit Court of Appeals refused to examine the documents, upholding the Government's motion for summary judgment. A petition for certiorari to the U.S. Supreme Court was denied. The Court of Appeals stated that "the question of what is desirable in the interest of national defense and foreign policy is not the sort of question that courts are designed to deal with."

Another case seeking judicial review under exemption (b)(1) in 1971 involved the right of access under the FOI Act to certain portions of the "Pentagon Papers." [83] Congressmen John E. Moss and Ogden R. Reid filed suit as individual citizens to enjoin Defense Secretary

[80] H. Rept. 92-1419, "Administration of the Freedom of Information Act," Sept. 20, 1972, p. 73.
[81] Hearings, "U.S. Government Information Policies and Practices—Administration and Operation of the Freedom of Information Act" (92d Cong., 2d sess.), pt. 4, pp. 1342-1343; p. 1347; pp. 1358-1359; pp. 1362-1363; pt. 6, pp. 2258-2259.
[82] *Epstein* v. *Resor*, 296 F. Supp. 214 (N.D. Cal. 1969), aff'd 421 F. 2d 930 (9th Cir. 1970, cert. den. 398 U.S. 965 (1970)). Professor Epstein testified before the Foreign Operations and Government Information Subcommittee on June 28, 1971, on the details of this case; see hearings, supra., pt. 2, pp. 285-308. A subsequent witness, Mr. William B. Macomber, Jr., Deputy Under Secretary of State for Administration, testified that the "Operation Keelhaul" file had not been declassified and made available by the U.S. Government because it was the joint property of our Government and the British Government and that their Government would not concur in its release; see hearings, supra., pt. 3, p. 924, see also hearings, pt. 2, p. 302 for text of White House letter confirming this fact.
[83] *Moss/Reid/Fisher* v. *Laird* (D.C. D.C. 1971) Civil Action No. 1254-71; see hearings, supra., pt. 4, p. 1363.

Laird from withholding classified portions of the "Pentagon Papers" and asked the U.S. District Court for the District of Columbia to examine the documents in camera. The Court refused and granted summary judgment for the Government.

In still another case, Representative Patsy Mink and 32 other Members of Congress requested in July 1971, documents pertaining to environmental reports of the Environmental Protection Agency and other Federal agencies on the planned underground nuclear test explosion on Amchitka Island, Alaska.[84] The U.S. District Court for the District of Columbia refused to compel disclosure of the documents, citing exemption (b)(1) and also (b)(5)—interagency memoranda.[85]

On appeal, the U.S. Court of Appeals reversed the District Court decision, remanding the case with instructions that the disputed documents be examined in camera to determine if any of the documents' components which were not classified for national defense purposes, or were not exempt as inter- or intra-agency memorandums, could be separated out and released.[86]

This decision was appealed by the Government, and the Supreme Court reversed the decision of the Court of Appeals. It decided that a claim of exemption under (b)(1) of the Freedom of Information Act was satisfied by affidavit of the Government that the documents were properly classified under the applicable Executive order and involved "highly sensitive matter * * * vital to our national defense and foreign policy." The court held that Congress has given to the Executive the power to determine if any information should be so classified and characterized, and that Congress did not intend to subject the soundness of executive security classifications to judicial review at the insistence of any objecting citizens. Because the Government had met its burden, through the above-mentioned affidavit, the fact of the classifications and the documents' characterizations never having been disputed by the respondents (Mink et al.), the duty of the District Court under section 552(a)(3) was therefore at an end. The court specifically negated the proposition that the exemption authorizes or permits in camera inspection of a contested document bearing a single classification so that the court might separate the secret from the supposedly nonsecret components and order disclosure of the latter.

The Supreme Court also upheld the Government's claim of exemption for three unclassified documents under exemption (b)(5) of the Freedom of Information Act (inter- or intra-agency memorandums). The Government should have, the court declared, an opportunity to support an exemption claim through expert testimony or other forms of evidence short of in camera inspection showing that the documents sought are of the sort clearly beyond the range of material that would be available to a private party in litigation with the Government agency. In camera inspection of all documents, is not, according to the court, "a necessary or inevitable tool in every case." But if the agency fails to meet its burden in claiming the (b)(5) exemption without in camera inspection, the court may order such inspection.[87]

[84] *Mink* v. *EPA*, 410 U.S.__(1973). Hearings, "U.S. Government Information Policies and Practices—Administration and Operation of the Freedom of Information Act" (92d Cong., 2d sess.), pt. 4, pp. 1362-1363. Background on the case may be found in testimony by Congresswoman Mink, hearings, pt. 8, pp. 3092-3101.
[85] Ibid.
[86] 464 F. 2.
[87] 410 U.S.__(1973). The opinion contains considerable discussion of the character of material in such inter- or intra-agency memorandums which could be regarded as exempt from disclosure under (b)(5).

Review of Classification System Ordered by President Nixon

After the eruption of the controversy over the publication of parts of the "Pentagon Papers" by the New York Times, Washington Post, and other newspapers, it was revealed that President Nixon had, on January 15, 1971, directed that "a review be made of security classification procedures now in effect." He established an "interagency committee to study the existing system, to make recommendations with respect to its operation and to propose steps that might be taken to provide speedier declassification." He later directed that "the scope of the review be expanded to cover all aspects of information security." [88]

Chairman of the interagency committee was William H. Rehnquist, then Assistant Attorney General, Office of Legal Counsel. The committee also had representatives of the National Security Council, the Central Intelligence Agency, the Atomic Energy Commission, and the Departments of State and Defense.[89] When Rehnquist was appointed to the Supreme Court in late 1971, the coordination responsibilities of the committee were assumed by Mr. David Young, Special Assistant to the National Security Council.

In related actions, the White House on June 30, 1971, issued an "administratively confidential" memorandum to all Federal agencies signed by Brig. Gen. Alexander M. Haig, Jr., Deputy Assistant to the President for National Security Affairs, ordering each agency to submit lists of the Government employees, outside consultants, and private contractors who hold clearances for access to top secret and secret information.[90]

Several days later, President Nixon then asked Congress to approve a $636,000 supplemental appropriation for the General Services Administration to assist the National Archives in the declassification of World War II records, which he estimated to total "nearly 160 million pages of classified documents." [91]

The interagency (Rehnquist) committee met sporadically during the summer and fall of 1971 and recommendations formulated by the committee were incorporated into a draft revision of Executive Order 10501. The draft was circulated for comment in January 1972 by the National Security Council to key departments and agencies most concerned with the security classification system.[92] But a request by Subcommittee Chairman Moorhead to White House Counsel John W. Dean III, for a copy of the draft for informal study and comment was denied.

The revised version of the NSC draft was issued by President Nixon on March 8, 1972, as Executive Order 11652, "Classification and Declassification of National Security Information and Material." [93] The new order, which superseded Executive Order 10501, had an effective date of June 1, 1972. A detailed discussion of Executive Order 11652 is in chapter VI, pages 52–87, and the text is contained in the appendix of this report.

[88] Statement by the President, The White House, Office of the Press Secretary, Mar. 8, 1972, p. 2, hearings, supra, pt. 3, p. 998.
[89] Hearings, supra, pt. 3, p. 780.
[90] Ibid., pt. 3, pp. 997–1000.
[91] H. Doc. 92–151; Congressional Record, Aug. 3, 1971, p. H7826.
[92] Hearings, supra, pt. 7, p. 2677; see also ibid., p. 2848.
[93] 37 F.R. 5200 (Mar. 10, 1972); the text of Executive Order 11652 and a section-by-section comparison of the new order with Executive Order 10501 is in pt. 7 of the hearings, pp. 2851–2883.

V. DIMENSIONS OF THE CLASSIFICATION PROBLEM

The broad scope of the increasingly difficult problem in dealing with the many facets of the security classification system came into sharper focus during the summer of 1971. The publication of the Pentagon Papers, and the subsequent attempts by the administration to invoke prior restraint against the printing of additional articles in the press based on these controversial top secret documents made millions of Americans more aware of the operation of the classification system. The 6 to 3 Supreme Court decision against the Government in the New York Times and Washington Post cases [94] and the depositions presented in those cases by both Government and outside classification experts revealed operational details of the system. Expert witnesses who testified at hearings by the House Foreign Operations and Government Information Subcommittee during the controversy uncovered other salient details as well as focusing attention on the growing Constitutional crisis affecting the right of Congress to obtain information from the executive branch.

Later leaks of Government documents during the India-Pakistan conflict in December 1971, the leak of a National Security Council memorandum early in 1972, revealing administration policy conflicts on Vietnam war strategy, and the continuing public attention on the Ellsberg-Russo trial in connection with the Pentagon Papers have all contributed to a broader understanding of the dimensions of the security classification problem.

The dimensions of the public policy and constitutional issues involved in the security classification problem were stated by President Nixon in his statement when he issued Executive Order 11652 on March 8, 1972: [95]

> The many abuses of the security system can no longer be tolerated. Fundamental to our way of life is the belief that when information which properly belongs to the public is systematically withheld by those in power, the people soon become ignorant of their own affairs, distrustful of those who manage them, and—eventually—incapable of determining their own destinies.
>
> Yet since the early days of the Republic, Americans have also recognized that the Federal Government is obliged to protect certain information which might otherwise jeopardize the security of the country. That need has become particularly acute in recent years as the United States has assumed a powerful position in world affairs, and as world peace has come to depend in large part on how that position is safeguarded. We are also moving into an era of delicate negotiations in which it will be especially important that governments be able to communicate in confidence.

[94] 403 U.S. 713; see hearings, supra, pt. 3, pp. 978-994 for text of decision.
[95] Hearings, supra, pt. 7; see pp. 2308-2328 for the complete text of the President's statement, the text of Executive Order 11652, and the text of the May 17, 1972, directive implementing the order.

> Clearly, the two principles of an informed public and of confidentiality within the Government are irreconcilable in their purest forms, and a balance must be struck between them.

Hearings were held by the House Foreign Operations and Government Information Subcommittee in May 1972 on security classification problems involving section 552(b)(1) of the Freedom of Information Act. They supplemented the subcommittee's June 1971 hearings on the "Pentagon Papers" and their relationship to the security classification system.[96]

When the subcommittee subsequently resumed its hearings on various aspects of the security classification system as part of its overall review of the operation of the Freedom of Information Act, Chairman Moorhead described the dimension of the problem in his May 1, 1972 opening statement: [97]

> There are 55,000 arms pumping up and down in Government offices stamping "confidential" on stacks of Government documents; more than 18,000 Government employees are wielding "secret" stamps, and a censorship elite of nearly 3,000 bureaucrats have authority to stamp "top secret" on public records.
>
> These are not wild estimates. These numbers were provided by the Government agencies, themselves. But even this huge number of Government censors is just the top of the secrecy iceberg.
>
> These Government officials are the ones who have been granted authority, under a Presidential order, to put "top secret," "secret," and "confidential" on Government records which are to be hidden from the public in the interests of national defense. It seems to me that this sort of national defense effort creates little more than a Maginot line made of paper—and it is even more dangerous than France's concrete and steel Maginot line which gave that country false confidence in its safety just before it was overrun by the German Army in World War II. * * *

In an article on "The Public's Right To Know," published in the January–February 1972, issue of Case & Comment, Representative Horton likewise pointed out that, "on balance, more emphasis is given in Executive Order 10501 to protection of classified material than to declassification of information that is no longer sensitive." He added: [98]

> This has resulted in much overclassification of information and a tremendous backlog, numbering in the millions of documents, of material which, while properly kept secret initially, should have been declassified years ago.

Many of the witnesses testifying at both the 1971 and 1972 hearings—from Government as well as outside experts—presented examples of specific abuses of the classification system as well as broadgage criticism of its overall operational shortcomings. Many of these specific cases are described in other sections of this report.

[96] Hearings, supra, pts. 1, 2, and 3.
[97] Hearings, supra, pt. 7, pp. 2283–2284.
[98] Hearings, supra, pt. 4, pp. 1032–1033.

But perhaps the most telling case against the security classification system as it operated under Executive Order 10501 for almost 20 years was made by President Nixon himself in this further quotation from his statement upon issuing Executive Order 11652: [99]

> Unfortunately, the system of classification which has evolved in the United States has failed to meet the standards of an open and democratic society, allowing too many papers to be classified for too long a time. The controls which have been imposed on classification authority have proved unworkable, and classification has frequently served to conceal bureaucratic mistakes or to prevent embarrassment to officials and administrations. * * *

Volume of Classified Material

The precise volume of classified documents that has accumulated in Government files was the subject of considerable inquiry during the subcommittee's hearings because of its important relationship to the overall scope of the classification problem. Various estimates were provided by governmental and outside witnesses.

Mr. William G. Florence, a retired Air Force security classification expert, with 43 years' Federal service, estimated that the Department of Defense had "at least 20 million classified documents, including reproduced copies." [100]

Later in the 1971 hearings, Mr. David O. Cooke, Principal Deputy Assistant Secretary (Administration), Department of Defense, was questioned by Congressman Horton on the 20 million figure: [101]

> Mr. HORTON. Mr. Cooke, I wanted to ask you, have you had an opportunity to read the statement of Mr. William Florence who testified before this committee last week?
>
> Mr. COOKE. Yes, I have read it once, sir.
>
> Mr. HORTON. In his statement on page 5 he makes this statement:
>
> > * * * the practice (overclassification) has become so widespread that the defense classification system is literally clogged with material bearing classification markings. I would guess that there are at least 20 million classified documents, including reproduced copies. I sincerely believe that less than one-half of 1 percent of the different documents which bear currently assigned classification markings actually contain information qualifying even for the lowest defense classification under Executive Order 10501. In other words, the disclosure of information in at least 99½ percent of those classified documents could not be prejudicial to the defense interests of the United States.
>
> Mr. HORTON. How do you react to that statement?
>
> Mr. COOKE. Mr. Horton, I am not a—Mr. Florence spent a long and distinguished career with the military in the Department of the Air Force, and I am not aware of the

[99] Hearings, supra, pt. 7, p. 2309.
[100] Hearings, supra, pt. 1, p. 97.
[101] Hearings, supra, pt. 2, p. 658.

factual basis or data which he used to express this purely personal judgment. We do not have any available figures on a defensewide basis. Classified documentation is used or is stored in active files and in DOD record-holding areas around the world. No reports are required at this time of the number of classified documents maintained by every DOD activity.

The closest we can come to it, sir, is biennial record reports indicating DOD holdings in total, classified and unclassified, of approximately 6 million cubic feet in active files. It was the estimate of one military department several years ago that 17 percent of the documents in their files were classified. If that figure is a valid estimate across the board, and we do not know whether it is, but assuming it is, I would say of our active record holdings, approximately 17 percent represent classified documents of all levels of classification. But I do not know the basis upon which the witness who appeared before you last week expressed that judgment. We have no data that we have been able to uncover which would support his assertion.

Mr. HORTON. Based on your knowledge of classified documents, from your position, how many would you estimate are classified?

Mr. COOKE. Based upon the collective judgment here, I would think, including reproduced copies, there could be more than 20 million classified documents. There is just no basis for reaching a judgment which could offer you any degree of reliable validity as to the precise number of documents.

Mr. HORTON. If you use the figure of 20 million, you would say there would be more than that?

Mr. COOKE. I would say there could quite possibly be more than 20 million classified documents, but I do not know. It could be less. As I said, the only approach we have to it was not by documents but by percentage of cubic feet of records and that was an estimated figure from one military department several years ago.

Mr. REID. What departments does that estimate you just made include?

Mr. COOKE. I believe the estimate of 17 percent was an estimate of the Department of Air Force.

The Defense Department supplied additional information on the magnitude of top secret documents: [102]

Centralized records are not maintained in the Department of Defense on the number of top secret documents which are declassified, or on the subject matter contained in such documents. The following general items of information, however, may be of interest:

1. In 1965, all elements of the Office of the Secretary of Defense reviewed all top secret documents in current files with a view to the elimination of the maximum possible number. There was an overall reduction of about 33 percent.

[102] Hearings, supra, pt. 2, p. 664.

The eliminated documents comprised 7,200 nonrecord documents destroyed, 1,700 retired to record centers, 49 downgraded, and nine declassified. In 1966, other elements of the Department of Defense made a similar review. Eight major elements reported. Of a starting total of over 1 million, 344,300 nonrecord documents were destroyed, 11,350 were retired to record centers, 9,000 were downgraded, and 710 were declassified, a reduction total of over 33 percent.

2. One major military command supplied the following figures derived from the annual classified document review of current file holdings. The figures are in linear feet. One linear foot represents 2,000 pages. A document may be one page or a thousand pages. A linear foot represents an average of 32 documents.

Top secret documents	1967	1968	1969
Destroyed (linear feet)	590	2,093	2,207
Downgraded (linear feet)	8	31	54
Declassified (linear feet)	1	0	210
Retired (linear feet)	0	0	0
Remaining (linear feet)	3,547	2,622	2,286

A conceptual idea of the volume of documents involved in the Defense Department's estimate of 6 million cubic feet was discussed during the hearings by Congressman Reid: [103]

> We have some expert mathematicians here on the committee, and they have taken your figures at face value, 6 million cubic feet of active files, and based on your possible estimate of 17 percent of these being classified are most favorable.
>
> The staff says that is about one-sixth or a million cubic feet, and it equals 18 stacks of documents 555 feet high, each as high as the Washington Monument.

The volume of classified documents in the State Department was discussed by two Department witnesses, who gave widely varying estimates. Deputy Assistant Secretary of State William D. Blair gave one figure in a colloquy with Congressman Moss: [104]

> Mr. Moss. Then this massive material, and you indicate in your statement that there are about 150 million documents in State. Mr. Blair——
>
> Mr. BLAIR. Yes, sir.
>
> Mr. Moss. One hundred fifty million previously classified.
>
> Mr. BLAIR. These are not all classified. This is classified and unclassified. But perhaps roughly one-quarter of them are classified.
>
> Mr. Moss. Thirty-five million documents classified under 10501 or prior to 10501?
>
> Mr. BLAIR. Well, not prior to 1945, Congressman Moss, because we have retired to the National Archives—that may not be quite completed, but we are in the process of retiring to the National Archives and opening up our files behind 1946. That is, through 1945. * * *

[103] Hearings, supra, pt. 2, p. 685.
[104] Ibid., pp. 2471–2472.

But testimony from Mr. William B. Macomber, Jr., Deputy Under Secretary of State for Administration, presented to the subcommittee in July 1971, gave a much lower estimate: [105]

> Mr. REID. How many documents are classified in the Department now; do you have any idea?
>
> Mr. MACOMBER. Well, yes, I can give you a rough idea. We have accumulated in our central files about 400,000 documents a year, of which about 200,000 are classified. So you can assume that we are accumulating classified documents at least at a 200,000-a-year rate.
>
> I looked historically to see, the other day, and the last 20 years we have accumulated at a rate, averaged about 100,000 classified documents a year over a 20-year period.
>
> Mr. REID. So we are talking of 2 million, roughly?
>
> Mr. MACOMBER. Yes, about 2 million, although the annual accumulation is greater now.

The most definitive estimates of the vast amount of classified documents in existence were presented by Dr. James B. Rhoads, Archivist of the United States.[106]

> In the last generation we have grown a great deal. We have become the National Archives and Records Service. We conduct an ongoing records management program working with agency officials and their files. We operate 15 Federal Records Centers and six Presidential Libraries, in addition to the National Archives itself. We have in our custody approximately 30 billion pages of Federal records, something more than 40 percent of the total volume of the Government's records. But while both our activities and our holdings have expanded, our goals remain the same: to serve the rest of the Government by caring for its noncurrent records and to serve the public in general by making available the documents of enduring value. * * *
>
> Perhaps, Mr. Chairman, a few statistics will demonstrate the dimension of this problem. We estimate that for the period 1939 through 1945 the National Archives and the several relevant Presidential Libraries possess approximately 172 million pages of classified material, including a small amount of material of permanent value in our Federal Records Centers. For the period 1946–1950 we estimate our classified holdings at approximately 150 million pages, and for the period 1950–1954 we estimate an additional 148 million pages. These estimates indicate that for the period from the beginning of the Second World War through the end of the Korean War we possess some 470 million pages of classified documents.

President Nixon, in his statement upon issuing Executive Order 11652, used similar figures in estimating the volume of classified documents for the World War II period through 1954: [107]

[105] Hearings, supra, pt. 3, pp. 905–906.
[106] Hearings, supra, pt. 7, pp. 2604–2605.
[107] Hearings, supra, pt. 7, p. 2309.

> Once locked away in Government files, these papers have accumulated in enormous quantities and have become hidden from public exposure for years, for decades—even for generations. It is estimated that the National Archives now has 160 million pages of classified documents from World War II and over 300 million pages of classified documents for the years 1946 through 1954.

Of course, relatively few classified documents originated later than 1954 have made their way into the National Archives, so that the almost half billion pages represents but a fractional part of the total volume of classified material presently in existence. It is virtually impossible for Government officials to make even a rough estimate of the total magnitude of even the original copies of such documents. And the problem is compounded when unknown numbers of reproduced copies are added to the total.

Authority To Classify

The volume of classified documents is directly related to the number of Government agencies and individuals within such agencies who are authorized to apply classification stamps. As noted earlier, Executive Order 10290, issued by President Truman in 1951, extended classification authority to all Federal departments and agencies. Agency regulations implementing the order extended uniform original classification authority to their employees. The proliferation of classification authority and the growth of the volume of classified material were taken into account by President Eisenhower when he superseded the Truman order in 1953 with Executive Order 10501. He denied original classification authority to 28 agencies and limited the authority in 17 others, including a number of Cabinet departments. Amendments to this order in subsequent years removed the authority to classify from several other agencies, as had been recommended by this committee.[108]

Under Executive Order 10501, as amended, 47 executive departments, agencies, boards, commissions, and offices eventually had authority to classify documents as top secret, secret, or confidential, including 10 units connected with the White House office. In 34 of these, where security classification was essentially linked to matters pertaining to the national defense, such authority could be delegated by the departmental or agency head. The authority was limited to the head of the other 13 departments and agencies which were not so closely related to the national defense.[109]

The Foreign Operations and Government Information Subcommittee's August 1971 questionnaire to executive departments and agencies solicited statistical data on the operation of the Freedom of Information Act. It also requested data on the numbers of employees authorized to classify under Executive Order 10501. The results of this study and a supplemental series of inquiries in January 1972 to 12 selected agencies having primary responsibility in the defense

[108] Report of the Commission on Government Security, op. cit., pp. 160–161. See also p. 18 of this report.
[109] Analysis of listing in section 2 of Executive Order 10501.

and foreign policy areas show that about 55,000 Government officials were authorized to classify documents or other material as top secret, secret, or confidential.[110]

The 55,000 total figure included 2,849 persons authorized to classify top secret, secret, and confidential and 18,029 persons authorized to classify secret and confidential. The remainder had confidential classification authority only. All of these figures refer to original classification authority.[111] The Department of Defense, including the Army, Navy, and Air Force, authorized 29,837 persons to classify under Executive Order 10501—783 top secret and 7,677 secret. The State Department, including the Agency for International Development, authorized 5,964 persons to classify—929 top secret and 2,155 secret. The Atomic Energy Commission authorized 6,173 persons to classify under the Executive order—310 top secret and 6,173 secret and confidential. None of these statistics, however, takes into account the extent of "derivative classification," the clerical reassignment or transfer of an existing classification of information contained in a document when portions of such classified documents are used in another document, report, or memorandum.

During the hearings, witness Florence provided the subcommittee insights into the extent to which "derivative classification" is a proliferating factor: [112]

> * * * (DOD Instruction 5210.47) delegates something called derivative classification authority to any individual who can sign a document or who is in charge of doing something.
>
> Such individual may assign a classification to the information involved if he believes it to be so much as closely related to some other information that bears a classification. This is called derivative classification authority.
>
> In the past several years I have not heard one person in the Defense Department say that he had no authority to classify information. The restrictions in Executive Order 10501 on delegating authority to classify have virtually no effect. * * *
>
> * * * The derivative classification practice is the serious problem in the Government today. Under this concept of derivative authority to classify, anyone can assign classifications, sir. Anyone. I used the statement, I believe, "hundreds of thousands" in my comments. * * *

[110] See analysis of questionnaire results by Congressional Research Service, Library of Congress, in appendix of hearings, supra, pt. 7, pp. 2929–2937. This figure does not include officials of the Central Intelligence Agency who are authorized to classify.

[111] "Original Classification" is defined in Department of Defense Instruction No. 5210.47 (Dec. 31, 1964) as follows:

Original Classification is involved when—

a. An item of information is developed which intrinsically requires classification and such classification cannot reasonably be derived from a previous classification still in force involving in substance the same or closely related information; or

b. An accumulation or aggregation of items of information, regardless of the classification (or lack of classification) of the individual items, collectively requires a separate and distinct classification determination.

See hearings, supra, pt. 1, p. 125.

[112] Hearings, supra, pt. 1, p. 98 and p. 104.

One of the most salutary results of the new Executive Order 11652 thus far observed is the reduction in both the number of agencies and the number of persons now authorized to exercise original classification authority. An August 3, 1972, statement from the White House Press Secretary's office, cited an oral report to the President by Ambassador John Eisenhower, Chairman of the Interagency Classification Review Committee, created by the new Executive order. The report indicates that the number of departments and agencies authorized to originally classify had been reduced to 25, excluding White House office agencies and that the number of persons having authority to originally classify information had been reduced by 63 percent—from 43,586 to 16,238.[113]

He indicated that top secret original classification authority had been reduced by 53 percent—from 2,275 to 1,076; secret by 39 percent—from 14,316 to 8,671; and confidential by 76 percent—from 26,995 to 6,491. These figures do not include the Central Intelligence Agency, which, according to the report made an overall reduction of 26 percent and a reduction in top secret of 84 percent. The April 1973 ICRC progress report, however, states that the number of top secret classifiers was reduced from 3,634 to 1,056 and that CIA top secret classifiers was reduced by 81 percent.

Overclassification Under Executive Order 10501

There has been virtually unanimous agreement—from the President on down—that serious abuses of overclassification had marked the operation of the security classification system under Executive Order 10501.

Defense Secretary Laird, speaking at the April 20, 1970, Associated Press luncheon in New York, said: "Let me emphasize my convictions that the American people have a right to know even more than has been available in the past about matters which affect their safety and security. There has been too much classification in this country." [114]

Former United Nations Ambassador and Supreme Court Justice Arthur Goldberg told the subcommittee: [115]

> Anyone who has ever served our Government has struggled with the problem of classifying documents to protect national security and delicate diplomatic confidences. I would be less than candid if I did not say that our present classification system does not deal adequately with this problem despite the significant advances made under the leadership

[113] The text of the statement and accompanying chart may be found in the hearings, pt. 7, pp. 2825-2827. Note the discrepancy between this figure and the total number of persons authorized to classify under Executive Order 10501, as reported the previous year by the agencies themselves in response to the subcommittee's questionnaire; that total was 55,000. An April 17, 1973, progress report of the Interagency Classification Review Committee used the figures 48,814 to 17,883.

Ambassador Eisenhower was appointed as Chairman of the newly established Interagency Classification Review Committee, authorized in sec. 7 of Executive Order 11652, on May 17, 1972. Other members of the Committee are the General Counsels of the State Department (John R. Stevenson), the Defense Department (J. Fred Buzhardt), the CIA (Lawrence R. Houston), the Justice Department (Ralph E. Erickson), and representatives of the Atomic Energy Commission (John V. Vinciguerra), and the National Security Council staff (David R. Young), who served as the Committee's Executive Director. Ambassador Eisenhower resigned as Chairman in April 1973; Executive Director Young of the NSC staff likewise departed that same month. By Executive Order 11714, issued by President Nixon on April 24, 1973, the Archivist of the United States was added to the Committee. Dr. James B. Rhoads, who currently holds that position, was named as Acting Chairman of the Committee. The text of this Executive order is in the appendix of this report.

[114] Hearings, supra, pt. 3, p. 975.

[115] Hearings, supra, pt. 1, p. 12.

of this committee and Congress in the Freedom of Information Act of 1966. I have read and prepared countless thousands of classified documents. In my experience, 75 percent of these documents should never have been classified in the first place; another 15 percent quickly outlived the need for secrecy; and only about 10 percent genuinely required restricted access over any significant period of time.

Moreover, whatever precautions are taken, leaks occur in a government of fallible men.

In short, the classified label in our experience has never been 100 percent respected.

William B. Macomber, Jr., Deputy Under Secretary of State for Administration, candidly stated: "We all know, I think, that there is a tendency in the executive branch to overclassify." [116]

Mr. Ralph E. Erickson, then Assistant Attorney General, Office of Legal Counsel testified: [117]

There is nearly universal agreement among those familiar with the operation of Executive Order 10501 that the existing system of classification has failed to strike the right balance between the public's need to know and the necessity to maintain certain information in confidence. The President put it well when he announced the issuance of the new order:

> Unfortunately, the system of classification which has evolved in the United States has failed to meet the standards of an open and democratic society, allowing too many papers to be classified for too long a time. The controls which have been imposed on classification authority have proved unworkable, and classification has frequently served to conceal bureaucratic mistakes or to prevent embarassment to officials and administrations.

Material classified under Executive Order 10501 and under preceding authorities has accumulated in vast quantities in Government files and storehouses. Only with the commitment of extensive Government resources can this mountain of classified material be reviewed or declassified within a reasonable period of time. Perhaps the chief deficiency of Executive Order 10501 was the failure of that order to provide an effective administrative system. Without an effective administrative system, its well-intended provisions turned out to be empty exhortations for the most part.

Classification expert William G. Florence, a retired Air Force security classification official with some 43 years of Federal service, testified: [118]

> I sincerely believe that less than one-half of 1 percent of the different documents which bear currently assigned classification markings actually contain information qualifying even for the lowest defense classification under Executive Order

[116] Hearings, supra, pt. 3, p. 902.
[117] Hearings, supra, pt. 7, p. 2678.
[118] Hearings, supra, pt. 1, p. 97.

> 10501. In other words, the disclosure of information in at least 99½ percent of those classified documents could not be prejudicial to the defense interests of the Nation.

In subsequent testimony, during the May 1972, hearings, Mr. Florence asserted that "the administrative security classification system currently in Executive Order 10501 is the source of most of the secrecy evils in the executive branch." He blamed loose implementation at the outset, and incredibly inept administration of the policy in recent years, (that) have invited and promoted widespread use of the three security classifications, "Top Secret," "Secret," and "Confidential." [119]

He went on to point out:

> The contagion of the classification philosophy long ago reached the point where the security system in Executive Order 10501 represents the greatest hoax of this century. Officials occupying even the highest positions in our Government have been conditioned to promote the belief that the words "top secret," "secret," and "confidential" on a paper automatically give it a substantive value of extraordinary importance, and beyond the ken of most people. * * *

Columnist Jack Anderson testified: [120]

> Not only does the executive branch sweep its bungles and blunders, its miscalculations and embarrassments under the secrecy labels, but our entire foreign policy and defense posture remains secret except for what the executive branch thinks is in its own interest to make available to the public. * * *
>
> It isn't just hush-hush Government activity that is classified. Newspaper clipping, public speeches and a wide variety of other public information have wound up with secrecy labels. When the Government went to court in its desperate bid to stop publication of the Pentagon papers by the Washington Post, the information cited as most sacrosanct repeatedly was shown by the Post to have already appeared in print. Ultimately, the Government itself acknowledged that there was "massive overclassification" of public papers.
>
> Does this mean there should be no Government secrets? Of course not. Our weapons technology, intelligence sources, and diplomatic contacts must be kept confidential. But the executive branch has used the classification system to censor the facts, to manage the news, to control the flow of information to the people.

Mr. William D. Blair, Jr., Deputy Assistant Secretary of State for Public Affairs, testified on the causes of the weaknesses of the security classification system established by Executive Order 10501: [121]

> As you know, Executive Order 11652 was the result of a year-long study of our system of handling national security information a study set in motion by President Nixon in

[119] Hearings, supra, pt. 7, p. 2531.
[120] Hearings, supra, pt. 7, pp. 2437–2438.
[121] Ibid., pp. 2463–2464.

January 1971, with a view to reform of that system. In these opening remarks I would like to summarize very briefly the principal conclusions which we, in the Department of State, drew from that year-long study—conclusions which I believe were broadly shared by our colleagues in the other agencies concerned—and which the new Executive order now reflects.

The first of these basic conclusions was simply this, that our existing system of classification and declassification, governed by Executive Order 10501, was not working as it should. Too much information, probably far too much, was being classified to begin with, and too much of that was being overclassified. In addition, the automatic declassification provision of Executive Order 10501 was virtually inoperative, since the language of the exceptions to it—particularly the definition of group 3—was so broad as to allow almost any classified document to be excluded from automatic declassification, and this privilege was being widely used or abused. * * *

He listed the following specific causes for the failure:

1. The system established under Executive Order 10501 was too complicated. The establishment of four groups for classification purposes, superimposed on three categories of classifications, required a list of definitions and rules which was hard to teach, hard to learn, and hard to remember. As a result, the terms of the order were widely misunderstood and even ignored.

2. This system as implemented gave too much authority to classify, and to exclude from automatic declassification, to too many people. This tended to insure a maximum flow of classified paper into the files, and a minimum return flow of automatically declassified paper out of the files.

3. The sheer volume of national security information, multiplying rapidly in the post-World War II period with the enormous expansion of our defense and foreign policy interests and programs has become so great that it simply overwhelms any declassification effort which is not largely and effectively automatic. * * *

4. Executive Order 10501 failed to provide an effective means of monitoring its implementation. And the handling of national security information, like any other large and complex undertaking, clearly requires leadership and management on a continuing basis if it is to be made to work.

These in my opinion were the essential conclusions to emerge from the interagency study which the President launched. I might add one more: the obvious fact that the conditions here suggested were contributing to a growing lack of respect, in and out of Government, for the classification system, with resulting damage both to the public's right to be informed and to its right to effective protection of its security interests.

95-678 O - 73 - 4

The implications of security classification abuses were clearly stated by David Wise, coauthor of "The Invisible Government," a critical study of the U.S. intelligence community:[122]

> Mr. Chairman, I believe that the central fact about the American political system today is that large numbers of people no longer believe the Government or the President, and I am speaking of any President. They no longer believe the Government because they have come to understand that the Government does not always tell the truth; that indeed it very often tells just the opposite.
>
> This erosion of confidence between the people and the Government is perhaps the single most important political development in America in the past decade. * * *
>
> President Nixon has recognized Government credibility as a continuing problem, and it is certainly not a problem associated only with the one administration or one political party. The American people have not been told the truth. If the people aren't told the truth, if they are misled, then I don't believe we can continue for very long to have a properly functioning democratic system. I think that there is obviously a very close relationship between public mistrust of Government, and of Government information, and the question of secrecy and document classification. I think that is very clear from the Pentagon study of the Vietnam war which led to the historic constitutional confrontation between the Federal Government, the New York Times and several other newspapers in recent days. Those materials make it clear that it is very simple for Government officials, by using the security classification system, to keep from public view policies, programs, plans, decisions and actions that are just the opposite of what the public is being told. In other words, we now have a system of institutionalized lying. Fortunately, no one has yet invented a rubberstamp or security classification that can keep the truth from eventually becoming known. But all too often, it does not become known quickly enough to inform the voters.

A similar theme was expressed by Senator Mike Gravel of Alaska in his testimony:[123]

> I think the cocoon of secrecy that we have woven over the years, particularly since the Second World War, is what has permitted us to go into Vietnam, permitted us to waste not only our blood, our young people, but also to waste our economic fiber. To what degree I don't think we will ever know. I think only history can judge that.
>
> I personally feel that our democracy is under assault, assault in a very unique way and in a very evolutionary way, and unless we can turn the tide we will lose the system of government we presently enjoy. And the single item that will

[122] Hearings, supra, pt. 2, pp. 329–330.
[123] Hearings, supra, pt. 7, p. 2553.

be responsible for this loss of government, this great experiment at self-government here in the United States, will be secrecy itself and nothing more, nothing more complex than that, because secrecy is anathema to democracy. It is that fundamental.

You can't ask people to go vote—and in our society the person who votes is supposed to be the final word—when secrecy prevails. It is a government of the people, by the people, for the people, so they have to give the final word. Quite obviously they can't vote intelligently or exercise their franchise with any efficiency if they don't know what they are voting about, and that depends upon the amount of knowledge they have.

Now, if that knowledge is spoon fed to them so they will arrive at preconceived conclusions, then obviously you develop a type of government that becomes first an autocracy and from there a dictatorship.

Congressman Otis Pike of New York, a member of the House Armed Services Committee testified: [124]

> The record of the Department of Defense in this area is uniformly on the side of secrecy. They have, in the past, been completely successful in getting Congress to approve weapons systems for which neither Congress nor the American public is told the ultimate cost, so why should they change.
>
> Far beyond classifying for purposes of national defense, they classify to change their testimony, to avoid embarrassment, and I expect most frequently through sheer stupidity and because no one ever tells them not to.
>
> We have all seen page after page after page of testimony stamped "secret," and then seen the Department of Defense release the same testimony with no change whatsoever. We have seen the biographies of generals and admirals stamped "secret." * * *
>
> In conclusion, it is my own judgment that 90 percent of what is classified should not be. Physically, there should be just as many people employed by the Pentagon declassifying material as there are classifying it. Their attitude has always been, "If in doubt—mark it secret." In a free society our attitude should always be, "If in doubt—tell the people the truth."

Historian Lloyd C. Gardner of Rutgers University observed:

> One can trace the growth of official secrets, both in volume and length of classification, with America's rise to "a powerful position in world affairs." As interest multiplied, so did secrecy. There is something uncomfortable in a democracy about that fact alone, something that bears close watching.[125]

[124] Ibid., pp. 2423–2424; an example illustrating unnecessary classification by the Navy of a 1969 letter to Congressman Pike, classified "Secret," by then Navy Secretary Chafee came out during the hearings. The letter, involving CTF 96 Op-Order 301–68 connected with the North Korean capture of the U.S. vessel *Pueblo*, had been included in the prepared text of Mr. Pike's May 1972 statement to the subcommittee. Subcommittee efforts to have it declassified by the Navy immediately prior to the hearings failed, but it was subsequently reviewed and declassified by Secretary Chafee during the course of Mr. Pike's testimony before the subcommittee; see hearings, pt. 7, pp. 2423–2425; 2433–2435.

[125] Ibid., pp. 2656–2657.

He went on to point out:

> Nations, like individuals, depend in part upon memory in order to be able to function rationally in the present. Historians are to a degree responsible for what stands out in a nation's memory; they supply experience longer than one generation's lifespan, and broader than that of any group of individuals.
>
> As one approaches the present, the historian's most valuable asset, perspective, is diminished chronologically, and in a secrecy-conscious nation, by the lack of available evidence as well.
>
> The Nation's memory is thus weakest for the years of the recent past, a serious defect, unless one is prepared to concede that the public should reach its conclusions on the basis of little or no information, or that the policymaker is the only one who needs the memory.

Other witnesses were more specific in their discussion of abuses in the security classification system, providing detailed information on cases of overclassification or needless classification that illustrates many of the basic shortcomings of Executive Order 10501.

Classification expert William G. Florence gave a number of examples in his testimony: [136]

> Some time ago, one of the service Chiefs of Staff wrote a note to the other Chiefs of Staff stating briefly that too many papers were being circulated with the top secret classification. He suggested that use of the classification should be reduced. Believe it or not, Mr. Chairman, that note itself was marked "top secret."
>
> The Air Force Electronics Systems Division at Hanscom Field, Mass., adopted the following statement for use on selected documents: "Although the material in this publication is unclassified, it is assigned an overall classification of confidential." We attempted some extra orientation in the Air Force regarding the definition of "confidential" at that time. I would not say our immediate success lasted very long. I still see practices of this sort.
>
> Not so very long ago, someone in the Navy Department placed the "secret" marking on some newspaper items of particular interest to the Navy. Subsequently, that action caused some embarrassment to the Department of Defense. As a result, a special directive had to be published to tell people not to classify newspapers. I see recently that practice within the Department of Defense is continuing anyway, the best I can tell from reading the newspapers today about the disclosures in the New York Times, the Washington Post, and the Boston Globe.
>
> A great many individuals in the Department of Defense, including highly placed officials, classify or strongly support the imposition of defense classifications on privately owned information, including privately generated applications for patents, regardless of the fact that Executive Order 10501

[136] Hearings, supra, pt. 1, pp. 99–100; other cases cited by Mr. Florence are found at pp. 98–103.

is clearly limited to official Government information. This really spreads classification beyond any possible control. And we can be certain that the tremendous costs which stem from this type of unnecessary classification, as well as all other unnecessary classifications, are charged to all of us as taxpayers.

Mr. Forrest M. Mims III, a former security officer at the Air Force Weapons Laboratory, Kirtland Air Force Base, N. Mex., also cited what he considered to be abuses of classification authority and procedures: [127]

Some examples of overclassification I observed at the Air Force Weapons Laboratory include the following:

1. In 1967, the Department of Defense classified a project to develop a personnel sensing system based on a principle of nature familiar to any school boy. Both the project and the principle were classified Top Secret (Special Access Required). The project was downgraded to a more reasonable classification level in 1970.

2. The Air Force classified as Secret (Special Access Required) a certain laser weaponry program because revelation of the weapon's target would result in revulsion and disapproval on the part of the general public. The project, though compromised on several occasions as a result of unclassified supporting experiments and studies, is still classified as Secret. An identical Army program, since discontinued as being impractical, was classified only Confidential.

3. An Air Force scientist invoked the classification system to prevent a research project from being transferred to an Air Force research laboratory with the assigned task of performing identical work but without the required security access. The classification system was invoked even though nearly all aspects of the project were treated as unclassified at the scientist's own laboratory.

While these examples of overclassification may seem inconsequential, they seriously impede the efficiency and communication necessary for high quality research.

Overclassification is by no means limited to Air Force research laboratories. I witnessed many examples of the practice elsewhere. For example:

1. In 1966, a brief lesson block on the history of the Bolshevik revolution taught at the Armed Forces Air Intelligence Training Center was classified Secret.

2. In 1967, a large selection of photographs showing atrocities wrought by communist troops against Vietnamese civilians was classified Confidential.

3. Also in 1967, aerial reconnaissance photographs taken by Air Force planes which revealed bombing of civilian structures in North Viet-Nam were classified Secret.

Congressman Michael J. Harrington of Massachusetts, a member of the House Armed Services Committee, said in his statement to the subcommittee: [128]

[127] Hearings, supra, pt. 3, p. 967.
[128] Hearings, supra, pt. 1, p. 227.

> But the military, by its constant penchant for secrecy, erodes whatever public confidence it may ever hope to have. The military has been sharply criticized lately, but instead of offering candid explanations for its policies, it hides behind the cloak of "Top Secret." I asked Secretary of the Navy Chafee why dumping at sea or the problems of race relations in the service were stamped "Confidential." While he agreed that the Navy should make every effort to bring dialog before the public, he explained that parts of the document were classified so all of it was classified.

Still other examples were provided by Mr. William G. Florence in his May 1972, testimony: [129]

> This subcommittee has an abundance of examples of unnecessary classification assignments showing that classification markings on a document usually are clearly unwarranted. I will describe only one at this time to emphasize how utterly ludicrous the classification system is in practice.
>
> Compilations of unclassified information are still being classified frequently by individuals who seem to believe that multiplicity or complexity itself should be protected. The Department of Defense affidavit given the court last summer in the Washington Post case involving the Vietnam study included the following: "It is sometimes necessary to classify a document in which no single piece or part is itself classified." This falsification of policy in Executive Order 10501 has led to unnecessary classification of millions of documents of the Department of Defense. * * *
>
> Another example of the classification of unclassified information is a document prepared by the Massachusetts Institute of Technology for the Air Force Space and Missile Systems Office, with the title, "Assembly Manual—Gyro Float." It was issued in February 1971 with the classification of confidential, which was the responsibility of the Air Force. Here is a copy of the document with the marking "confidential" on the cover. This document, with its confidential classification marking, contains the following statement:
>
> > Each section of this volume is in itself unclassified. to protect the compilation of information contained in the complete volume, the complete volume is confidential.
>
> Also in the foreword of the document is the following statement, which is required by Executive Order 10501 on all classified documents held by contractors and others outside the executive branch:
>
> > This document contains information affecting the national defense of the United States within the meaning of the Espionage Laws, title 18, United States Code, sections 793 and 794, the transmission or revelation of which in any manner to an unauthorized person is prohibited by law.

[129] Hearings, supra, pt. 7, pp. 2533-2534.

> This nonsensical practice of the Department of Defense not only is outrageously expensive in terms of wasted money but it is atrocious in its application to individuals who happen to become involved in an allegation of mishandling the unclassified information. I have seen people in responsible positions blindly take punitive action against employees in the Government and in industry for handling such unclassified information as being unclassified.

One opinion showing the widespread extent of abuse in the security classification system was presented by Gene R. LaRocque, rear admiral (retired), U.S. Navy, a much-decorated veteran of 31 years of naval service. He testified:[130]

> In the military the best way to prevent disclosure of information is to classify it. Classification is made for a variety of reasons. First, to prevent it from falling into the hands of a potential enemy; this is legitimate but accounts for only a small portion of the material classified. Other reasons for classifying material are: to keep it from the other military services, from civilians in their own service, from civilians in the Defense Department, from the State Department, and of course, from the Congress. Sometimes, information is classified to withhold it for later release to maximize the effect on the public or the Congress.
>
> Frequently, information is classified so that only portions of it can be released selectively to the press to influence the public or the Congress. These time released capsules have a lasting effect.* * *

Admiral La Rocque also stated:

> Regrettably, far too much material is classified, much of it just because it is easier to classify than not. You cannot get into trouble by overclassifying, only by failing to classify. And, it is easier to maintain secure files if all material is classified. In that way, only one set of files need be maintained.
>
> Classification is also very simple; all one needs is a typewriter or a Secret stamp. In most offices, the secretaries or the yeomen establish the classification. And since most typed matter is not signed, no one ever knows who classified the material or for what reason. There is no central record of what was classified by whom, when, or for what purpose.

Costs of the Security Classification System

Considerable attention was focused during the hearings on the cost to the American taxpayers in the operation of the security classification system.

Retired Air Force security classification expert William G. Florence testified that:[131]

> There is a massive wastage of money and manpower involved in protecting this mountainous volume of material with unwarranted classification markings. Last year, I estimated that about $50 million was being spent on protective

[130] Hearings, supra, pt. 7, pp. 2909–2910.
[131] Hearings, supra, pt. 7, p. 2532.

> measures for classified documents which were unnecessarily classified. After further observation and inquiry, and including expenditures for the useless clearances granted people for access to classified material, it is my calculation that the annual wastage for safeguarding documents and equipment with counterfeit classification markings is over $100 million.

In response to the subcommittee's request for cost data, the Defense Department subsequently furnished a statement for the record which provided some representative costs for various components of the system. However, the Department said that:

> There are no available data on the total costs which could be attributed to security classification or to the protection and handling of classified documents and material.[132]

Among the types of "representative costs" noted by DOD, was data showing the use of 175 man-months to review 240,000 World War II classified documents representing over 1,800,000 pages and the declassification of over 100,000 of them at an average cost of 66 cents per document. In the handling, protecting, and transmission of classified documents, DOD estimates that it presently costs $2.57 for handling a top secret document in transit. They also estimate that it presently costs 36 cents per top secret document in conducting the required annual inventories of such documents within DOD.

In an effort to obtain more precise estimates of security classification costs, Subcommittee Chairman Moorhead requested the assistance of the General Accounting Office in a June 29, 1971, letter to Comptroller General Staats. Subsequent meetings of the subcommittee and GAO staffs developed reasonable guidelines of the types of information to be included in the GAO study, which was completed and delivered to the subcommittee on February 16, 1972, and printed in the hearing record (B–173474).[133]

The study focused on all aspects of security classification costs, including management and policy, classification and declassification, training, transmitting, safeguarding, administering, and enforcing security policies, counterintelligence activities related to document security, and the costs of personnel investigations. Four Federal agencies having major security classification responsibilities were included in the study—the Departments of State and Defense, the Atomic Energy Commission, and the National Aeronautics and Space Administration. Total estimated expenditures during fiscal 1970 for State, DOD, and NASA, and during fiscal 1971 for AEC were $60.2 million.[134]

The $60.2 million estimate is only a fraction of the total expenditures within these four departments and agencies, however, because security costs associated with the performance on Government classified contracts are not identified separately. In his response to GAO, DOD Assistant Secretary Robert C. Moot stated:[135]

[132] Hearings, pt. 2, pp. 690–691; all figures used here are contained in this referenced statement provided by the Defense Department.
[133] Hearings, supra, pt. 7, pp. 2286–2293.
[134] Ibid., p. 2287. An additional $66.1 million indirectly related to the classification system was spent for personnel security investigations.
[135] Hearings, supra, pt. 7, p. 2290.

G. Security Costs Included in the Price of Government Contracts

1. Estimated fiscal year 1970 cost: Not available.

2. Comment: The security costs associated with the performance on Government classified contracts are embodied in "overhead" and are not separately identified. The identification of such costs could be obtained on a sampling basis with the voluntary participation of industry. Time and resources do not permit this kind of a survey. However, based on a limited survey of 10 contractors handling 30 contracts, one component reported that of a total of $54,200,000 of R.D.T. & E. funds obligated by that component in fiscal year 1970, it estimates that $380,200 or 0.7 percent of contract price was attributed to security costs. In these cases, security cost on a percent of contract price ranged from 0.2 to 2.2 percent: however, security cost for only two of the 10 industrial firms exceeded 1 percent.

While this sample cannot be totally relied upon for accurate security cost figures, it is noted that DOD's total research development test and evaluation obligations for fiscal 1970 were some $7 billion out of a $36 billion in total contract awards by DOD that year. If the same 0.7 percent estimate used above were applied to the total R.D.T. & E. spending, as much as $49 million might be added to DOD security classification costs.

Other security classification-related costs are also left out of the $60.2 million figure. State Department data on classification management and associated classification and declassification activities are "not substantial," according to Richard W. Murray, Deputy Assistant Secretary for Budget and Finance. The Defense Department gave no figure for administration and enforcement of security policies, procedures, and regulations; neither did AEC or NASA.[136] Thus, each of the four agencies could not even provide estimates to GAO in at least two or more of the categories of estimates requested.

It should also be noted that these cost estimates provided in the GAO study are based on experience under Executive Order 10501, not the new Executive Order 11652 that was issued in March 1972.

[136] Ibid., p. 2287.

VI. EXECUTIVE ORDER 11652 ISSUED BY PRESIDENT NIXON

As noted earlier, President Nixon issued Executive Order 11652 on March 8, 1972, the end-product of more than a year of study and drafting by the interagency committee which operated under the guidance of the National Security Council. The new order, entitled "Classification and Declassification of National Security Information and Material," was accompanied by a statement that detailed the abuses and shortcomings in the security classification system documented over the years by hearings and reports of this committee.[137]

The preamble of the Executive order directly links the authority for its issuance to the Freedom of Information Act: [138]

> The interests of the United States and its citizens are best served by making information regarding the affairs of Government readily available to the public. This concept of an informed citizenry is reflected in the Freedom of Information Act and in the current public information policies of the executive branch. * * *
>
> This official information or material, referred to as classified information or material in this order, is expressly exempted from public disclosure by Section 552(b)(1) of Title 5, United States Code. Wrongful disclosure of such information or material is recognized in the Federal Criminal Code as providing a basis for prosecution.

Executive Order 11652 had an effective date of June 1, 1972, but the implementing guideline directive for regulations was not issued until May 17, 1972, and initial regulations were not published until August 3, 1972—over 2 months after the effective date.[139]

Questions of Timing of the New Order

On January 24, 1972, the committee issued a press release announcing plans for a series of hearings on the administration of the Freedom of Information Act to begin in early March, to include, among various related subject areas, an investigation of the Government's security classification system.[140] The announcement came during the final review stages by the National Security Council and executive agencies of the draft revision of Executive Order 10501 described earlier at page 31 of this report.

[137] See p. 105 in appendix of this report for text of the order.
[138] Hearings, supra, pt. 7, p. 2312.
[139] 37 F.R. 15624 et seq. (Aug. 3, 1972), for texts of regulations of the Atomic Energy Commission, the Central Intelligence Agency, the General Services Administration, and the Departments of State, Defense, and Justice.
[140] Hearings, pt. 4, pp. 1021-1022.

A two-part article by Mr. Sanford Ungar of the Washington Post appeared on February 11 and 12, 1972, which described in detail the provisions of the draft security classification Executive order.[141] The article stated that a copy of the draft had come into the possession of the Post. Efforts were made that same day by the subcommittee staff to obtain a copy from the Office of Legal Counsel, Department of Justice, for informal review and comment. The request was denied by an official at the Justice Department, who asserted that the document was "only a working draft," although the Post story had stated that its transmittal letter had called it "the final draft." A subsequent request by Subcommittee Chairman Moorhead to White House Counsel John W. Dean III, for a copy of the draft for such purposes was also denied a few days later.

Several weeks later, in remarks on the House floor, Subcommittee Chairman Moorhead recounted efforts to obtain a copy of the draft order and cited the subcommittee's long experience in the security classification field and the legislative alternative being worked on by the staff to replace Executive Order 10501. He also mentioned "rumors that had been circulating" about the planned issuance of a new Executive order to preempt congressional action in this area. Subcommittee Chairman Moorhead also cautioned against hasty action because of what seemed to be serious inadequacies and defects in the draft, as described in the Ungar articles.[142] The new Executive Order 11652 was issued a week later on March 8. Its issuance was promptly deplored as premature by Mr. Moorhead in remarks on the House floor.[143]

The subcommittee staff was directed to make an intensive study and analysis of the new order, comparing its provisions on a section-by-section basis with Executive Order 10501. The analysis was completed the following week and the full text was placed in the Congressional Record on March 21, 1972.[144] While praising the President's statement that accompanied the new order, describing the dimensions of the security classification problem, Mr. Moorhead listed in his remarks in the Record a number of its major defects as revealed in the subcommittee staff analysis. Witnesses from the executive branch who testified during the May 1972 subcommittee hearings were requested to comment on these specific defects so that any misinterpretations of the precise meaning of the language of these sections of the new Executive order could be clarified on the record.

The major points in dispute are discussed later in this chapter.

Not only had the executive branch refused the subcommittee's request for an opportunity to informally review and comment on the proposed draft of the new Executive order, but it also refused to permit testimony by Mr. David Young, a special assistant to the National Security Council, who had assumed major responsibility for coordi-

[141] Hearings, pt. 7, pp. 2303–2306 contain the text of the two Washington Post articles by Mr. Ungar; his description of various provisions of the draft are quite accurate when compared to the actual text of the new order issued the following month.

[142] Congressional Record (Mar. 1, 1972), p. H1637, hearings, pt. 7, pp. 2844–2845. See hearings, pt. 7, pp. 2303–2306 for text of Ungar articles in Washington Post; see also pp. 2527–2528 for description of sequence of events.

[143] Congressional Record (Mar. 8, 1972), p. H1892; hearings, pt. 7, p. 2848–2849.

[144] Congressional Record (Mar. 21, 1972), p. E2774; text also in hearings, pt. 7, pp. 2849–2883.

nating work on the final draft of the Executive order by the interagency committee when its chairman, Assistant Attorney General Rehnquist, was appointed to the Supreme Court. A subsequent request for the opportunity to review the draft directive implementing the new Executive order was also refused. Subcommittee Chairman Moorhead described the sequence of events in his opening statement at the May 2, 1972, hearing in which the subcommittee received testimony from State and Defense Department officials on the new Executive order: [145]

> We had also invited here today Mr. David Young, special assistant to the National Security Council, who is considered by some to be the major architect of the new Executive Order 11652. At the conclusion of my statement, I will insert into the record the letter which I wrote to Mr. Young on April 24, inviting him to testify. Citing the Flanigan precedent involving the ITT investigation, I had offered, in behalf of subcommittee, the agreement not to pose questions that "might tend to impinge on your personal discussions with the President in this area (of the Executive order)."
>
> Unfortunately, Mr. Young is not here today. This morning I received a letter from Mr. John Wesley Dean III, a counsel to the President, asserting so-called Executive privilege.
>
> Mr. Young's office was also requested to supply to this subcommittee a copy of the guideline directive for implementation of the Executive Order 11652, which he has prepared for the executive departments and agencies affected by the new Executive order.
>
> This morning, in a telephone conversation, Mr. Young declined at this time to submit this implementation order to the subcommittee. I told Mr. Young that I thought this was unfortunate, that there should be greater cooperation between the executive branch and the legislative branch and that I thought that our studies and our hearings had given this subcommittee a degree of expertise that would help in the drawing up of an effective implementation order. I also suggested that if we had been permitted to participate in the drafting of this directive we would be in a position where we could not be too critical, unless we told them ahead of time that we had certain points of reservation.
>
> Unfortunately, this degree of cooperation which we have offered has not been accepted by the White House, and this is particularly regrettable because the matters we are discussing here are of the highest importance to this subcommittee and to the Congress as a whole.

In his opening statement at the May 3, 1972, hearing, Subcommittee Chairman Moorhead deplored the lack of specific rebuttal by executive branch witnesses to allegations of defects and loopholes in the new Executive order made in the subcommittee's analysis and also raised the question of timing of the June 1 effective date of the new order: [146]

[145] Hearings, pt. 7, pp. 2451-2452; text of correspondence with Mr. Young and White House Counsel John W. Dean III is on pp. 2452-2453; later in the May 2 hearing, Chairman Moorhead placed in the hearing record the text of a White House press conference in which Mr. Young answered some of the types of questions posed by news reporters that would have been put to him by subcommittee members; see ibid., pp. 2505-2515.
[146] Ibid., p. 2528.

> * * * another serious problem was also raised at the hearings yesterday. The subcommittee learned from Mr. J. Fred Buzhardt, General Counsel of the Defense Department, and from Mr. William D. Blair, Assistant Secretary of State, that the National Security Council has not yet issued its guideline directive to departments and agencies affected by the new Executive order. This is despite the fact that the new order is to take effect on June 1, less than 28 days from now. No departmental or agency directives or regulations can be written until such guidelines are received. Even after they are drafted, they must be reviewed, cleared, printed, promulgated, and physically delivered to U.S. military and diplomatic stations in the far-off corners of the globe. Moreover, since the new order differs greatly from the old in some respects, extensive familiarization and training of personnel will be required to make it fully effective in safeguarding the legitimate security interests of our national defense and foreign policy.

In order to assure the opportunity for an orderly review of the adequacy of Executive Order 11652 in safeguarding our essential national secrets and to provide time for its proper implementation, Mr. Moorhead urged the indefinite suspension of its effective date: [147]

> I am, therefore, calling on the President of the United States to indefinitely suspend the effective date of the new Executive order. Its inherent defects and the lack of time to fully implement it make it imperative that he act promptly to prevent further chaotic conditions that could adversely affect our national defense and foreign policy.
>
> While the existing Executive Order 10501, governing the security classification system is far less than perfect, it has been in effect since 1953. The hasty, ill-conceived replacement classification system provided for in the new Executive order is not the answer. The delay in the effective date of any new system would be a rational approach and in the national interest.

No response to the request for suspension of the new Executive order's effective date was forthcoming from the White House. The National Security Council's guideline directive for implementation of Executive Order 11652 was not published until May 19, 1972,[148] and the first departmental and agency regulations were not promulgated until August 3, 1972—more than 2 months after the effective date of the new Executive order.[149]

In its haste to undercut congressional investigation of the security classification system by the issuance of a faulty Executive order without allowing adequate time for the preparation, review, dissemination, and training under new implementing regulations, the Nixon administration may have seriously impaired the effective functioning of the entire classification system. The question of legality

[147] Ibid., this action was also called for by Chairman Moorhead in a speech on the House floor on May 3, 1972, Congressional Record, p. H4093; for text see hearings, pt. 7, pp. 2889–2890.
[148] 37 F.R. 10053; for text of directive, see hearings, pt. 7, pp. 2319–2328.
[149] 37 F.R. 15624; for text of regulations of the State, Defense, and Justice Departments, the Atomic Energy Commission, the Central Intelligence Agency, and the General Services Administration, see hearings, pt. 7, p. 2329.

of classification markings applied in some cases under the old Executive Order 10501 during the hiatus between June 1, 1972, and August 3, 1972, is discussed later in this chapter.[150]

Major Features of Executive Order 11652

In his March 8, 1972, statement accompanying the new Executive order, President Nixon outlined its "most significant features" as follows:[151]

> The rules for classifying documents are more restrictive.
>
> The number of departments and people who can originally classify information has been substantially reduced.
>
> Timetables ranging from 6 to 10 years have been set for the automatic declassification of documents. Exceptions will be allowed only for such information as falls within four specifically defined categories.
>
> Any document exempted from automatic declassification will be subject to mandatory review after a 10-year period. Thus, for the first time, a private citizen is given a clear right to have national security information reviewed on the basis of specified criteria to determine if continued classification is warranted so long as the document can be adequately identified and obtained by the Government with a reasonable amount of effort.
>
> If information is still classified 30 years after origination, it will then be automatically declassified unless the head of the originating department determines in writing that its continued protection is still necessary and he sets a time for declassification.
>
> Sanctions may be imposed upon those who abuse the system.
>
> And a continuing monitoring process will be set up under the National Security Council and an interagency classification review committee, whose chairman is to be appointed by the President.

A White House "Fact Sheet on Executive Order 11652," issued on August 3, 1972, lists "the three basic objectives of the new Executive order as: (1) To reduce the amount of material classified by the Government; (2) to provide for speedier declassification under automatic schedules; and (3) to insure implementation of the order through the establishment of an Interagency Classification Review Committee."[152]

Key executive branch witnesses also commented on the scope and objectives of the new Executive Order 11652 in their testimony. Defense Department General Counsel J. Fred Buzhardt said:[153]

> Executive Order 11652 represents a significant milestone in the efforts of the executive branch to provide a rational balance between the public's right to know about the affairs

[150] See p. 80 of this report. Initial regulations were issued on Aug. 3, 1972.
[151] Hearings, pt. 7, p. 2310; for texts of President Nixon's statement, and the text of Executive Order 11652 see ibid., pp. 2308–2319.
[152] Progress report on implementation of new order contained in press release, Office of the White House Press Secretary, Aug. 3, 1972; for text, see hearings, pt. 7, pp. 2826–2827.
[153] Ibid., p. 2454; see also a chart presented by Mr. Buzhardt comparing major features of the old and new Executive orders, pp. 2461-2462.

> of Government, and the equally compelling need to protect certain information against unauthorized disclosure. The Department of Defense is working with an enthusiastic commitment to implement the new policies in order to correct deficiencies in the existing system and to confine classification to that information which truly requires protection in the interest of national security, and to continue that classification only for the minimum time absolutely required. In short, the Department of Defense is dedicated in dealing with known problems in the classification system forthwith and to overcoming any potential roadblock to speedy progress.

Mr. William D. Blair, Jr., Deputy Assistant Secretary of State for Public Affairs and a member of the committee that drafted the new Executive order, outlined in his testimony the major causes of the failure of Executive Order 10501. He indicated ways in which the new order was intended to meet "each of the serious weaknesses" of the old order: [154]

> First, the elimination of the complicated and ineffective group system has somewhat simplified the new order, in comparison with its predecessor. While a list of exemptions from automatic declassification remains, it is specific in nature and more restricted in scope.
>
> Second, the authority to classify, and the authority to exempt from automatic declassification, have been sharply restricted in terms both of numbers and agencies and numbers of individual officers.
>
> Third, the effect of these changes, and of other changes in the new order, will be to provide for the first time a declassification system which is genuinely automatic. While the need for individual review of specific documents in specific cases will always remain, the principle is here established that all material will be declassified when the calendar reaches the declassification date typed or stamped on the face of each document: and for the great bulk of material, this will occur in accordance with a standard and shortened declassification schedule which ranges from 6 to 10 years according to classification categories.
>
> Fourth, Executive Order 11652 establishes a practical framework for monitoring the implementation of the new system on a continuing basis, under the broad supervision of a high-level interagency classification review committee, acting for the National Security Council, and of a senior-level group in each department.

Mr. Ralph E. Erickson, then Assistant Attorney General, Office of Legal Counsel, described the "chief deficiency" of Executive Order 10501 as follows: [155]

> Material classified under Executive Order 10501 and under preceding authorities has accumulated in vast quantities in Government files and storehouses. Only with the commitment of extensive Government resources can this mountain of classified material be reviewed or declassified within a

[154] Ibid., pp. 2464–2465.
[155] Ibid., p. 2678.

reasonable period of time. Perhaps the chief deficiency of Executive Order 10501 was the failure of that order to provide an effective administrative system. Without an effective administrative system, its well-intended provisions turned out to be empty exhortations for the most part.

He then went on to comment on Executive Order 11562:

Since the issuance of the new order there has been extensive comment and testimony on whether the new order will in fact limit the volume of classified material and bring about a significant increase in the amount of information available to the public. While only time will tell whether the new approaches embodied in Executive Order 11652 will succeed where the old approaches failed, we are sanguine. The new order reflects the judgment of experienced persons in the security field with a lively appreciation of the bureaucratic problems and pressures that resulted in the shortcomings of the old system. Clearly no system, no matter how well devised, will bring about significant changes unless the people operating and supervising it are committed to its goals. We believe that the rules and machinery set up by the new order provide an excellent framework within which the executive branch can work toward its goal of cutting back sharply on the quantity and duration of security classification.

The Archivist of the United States, Dr. James B. Rhoads, discussed the portions of the new Executive order that would particularly affect the operations of the National Archives in their declassification efforts. He also stated: [156]

* * * We in the National Archives are particularly sensitive to the problems involved with classified documents. From our point of view Executive Order 11652 is a decided improvement over the earlier Executive order. It attempts to strike a new and better balance between the Government's need for confidentiality and the people's right to know—a balance in favor of greater access.

Conflicting Interpretations of Key Sections of New Order

A number of major problem areas representing conflicting interpretations of key provisions of Executive Order 11652 were discussed during the hearings. Many of these areas of contention were outlined in the subcommittee staff analysis of Executive Order 11652 and the section-by-section analysis of the old and new Executive orders mentioned earlier. The 11 alleged defects were that it: [157]

(1) Totally misconstrues the basic meaning of the Freedom of Information Act (5 U.S.C. 552);

(2) Confuses the sanctions of the Criminal Code that apply to the wrongful disclosure of classified information;

(3) Confuses the legal meaning of the terms "national defense" and "national security" and the terms "foreign policy" and "foreign relations" while failing to provide an adequate definition for any of the terms;

[156] Ibid., p. 2608.
[157] Ibid., p. 2850.

(4) Increases (not reduces) the limitation on the number of persons who can wield classification stamps and restricts public access to lists of persons having such authority;

(5) Provides no specific penalties for overclassification or misclassification of information or material;

(6) Permits executive departments to hide the identity of classifiers of specific documents;

(7) Contains no requirement to depart from the general declassification rules, even when classified information no longer requires protection;

(8) Permits full details of major defense or foreign policy errors of an administration to be cloaked for a minimum of three 4-year Presidential terms, but loopholes could extend this secrecy for 30 years or longer;

(9) Provides no public accountability to Congress for the actions of the newly created Interagency Classification Review Committee;

(10) Legitimizes and broadens authority for the use of special categories of "classification" governing access and distribution of classified information and material beyond the three specified categories—top secret, secret, and confidential; and

(11) Creates a "special privilege" for former Presidential appointees for access to certain papers that could serve as the basis for their private profit through the sale of articles, books, memoirs to publishing houses.

A number of these major defects in the new Executive order are discussed in the following portion of this chapter.

Statement in the Preamble of Executive Order 11652

The first series of criticisms in the subcommittee staff analysis was directed at certain statements contained in the preamble of the new Executive order. The first of these involved references to the Freedom of Information Act. The third paragraph of the preamble reads: [158]

> This official information or material, referred to as classified information or materials in this order is expressly exempted from public disclosure by section 552(b)(1) of Title 5, United States Code. Wrongful disclosure of such information or material is recognized in the Federal Criminal Code as providing a basis for prosecution.

The use of the term "expressly exempted" implies that all exemptions under the Freedom of Information Act are mandatory upon executive agencies in responding to a request for information under the act. In reality, the use of such exemptions are permissive only. Thus information subject to exemption (b)(1) could be declassified and made public upon request.

A subsequent colloquy during the hearings between then Assistant Attorney General Erickson and the subcommittee staff director dealt with the term "expressly exempt" and the language of the preamble referring to the Freedom of Information Act. Mr. Erickson readily admitted that "the exemptions (under the Freedom of Information Act) are permissive in the sense that there is nothing in the

[158] Ibid., p. 2851.

act that would prohibit an executive agency or department from disclosing records coming within them." He defined the term "expressly exempt" as having the option to disclose it.[159]

The reference to the Federal Criminal Code in the last sentence of paragraph three of the preamble was also the subject of contention. Prosecutive action for an alleged "wrongful disclosure" of classified information or material described in Executive Order 11652 would be proper only if it met the test of the types of information specifically referred to in the criminal code, not necessarily that specified in the Executive order, and if the purpose or conditions of the alleged "wrongful disclosure" met the additional tests as contained in the code and court decisions based on those sections. There is no basis in law for an Executive order, in effect, to threaten Members of Congress, newsmen, or anyone else for what the order refers to as a "wrongful disclosure."

This point was discussed in a colloquy between Subcommittee Chairman Moorhead and Mr. Erickson during his March 10, 1972, testimony on the administration of the Freedom of Information Act:[160]

> Mr. MOORHEAD. Under the Executive order, the duty of interpretation is assigned to the Justice Department, is it not?
>
> Mr. ERICKSON. Yes, it is. The Attorney General has that responsibility under section 7C, I believe it is.
>
> Mr. MOORHEAD. I notice in the Executive order, in the third paragraph, it refers to exemptions under section 552(b)(1) of title 5, which is the Freedom of Information Act, and it says "wrongful disclosure of such information or material is recognized in the Federal Criminal Code as providing a basis for prosecution."
>
> What is the meaning of the word "wrongful" there?
>
> Mr. ERICKSON. Wrongful in that context, to me, would mean disclosure of a classified document to one who is not entitled to receive it.
>
> Mr. MOORHEAD. Therefore, you would say that disclosure of such information would not require intent to harm the United States?
>
> Mr. ERICKSON. I would refer you to the particular statutes involved, and I was just giving you my broad interpretation of what wrongful would mean. I would have to relate that to the criminal statutes involved, both in title 18, and there is a statute in title 50 also which would cover this situation. I am sure that is the reference.
>
> Mr. MOORHEAD. So that "wrongful" in this context would be wrongful as defined in the criminal statutes, not as defined in the Executive order, is that correct?
>
> Mr. ERICKSON. That would be my understanding.
>
> Mr. MOORHEAD. Because an Executive order cannot create a criminal offense, is that not correct?
>
> Mr. ERICKSON. Yes, sir.

[159] Ibid., pp. 2702-2703.
[160] Hearings, pt. 4, p. 1185.

> Mr. MOORHEAD. So that this Executive order just as the previous 10501 does not in and of itself create a law, a violation of which is a criminal offense?
>
> Mr. ERICKSON. That is correct.
>
> Mr. MOORHEAD. I think that that is important, because as you said before, the exemptions under the Freedom of Information Act are not directives, but are merely permissive. Therefore, if we construe this paragraph to make these disclosures of exempt items a violation, we are really misconstruing what you so ably testified were options rather than directions. This uncertainty which is created, that is, that mere disclosure of classified information, without the required intent under the criminal laws, is not in and of itself a criminal violation. * * *

The same point was also discussed later in the hearings. Deputy Assistant Attorney General Kevin Maroney, head of the Internal Security Division, had used similar terminology in a speech at the annual convention of the American Society of Newspaper Editors on April 19, 1972. His remarks were construed by some to give the appearance of threatening newsmen with criminal prosecution if they should publish information bearing a classification marking.[161] Mr. Maroney appeared at the subcommittee hearing to discuss the allegation and denied that he had meant to threaten those in attendance. He also conceded, however, that the reference in Executive Order 11652 to the criminal code could not broaden the scope of the statute.[162] Mr. Erickson also made it clear that this language of the Executive order was not intended "to establish any criminal sanction." [163]

National Defense Versus National Security

Another major provision of Executive Order 11652 examined in the hearings was the change in terms in section 1, "Security Classification Categories" from that of the old Executive order. Executive Order 10501 used the term "interests of national defense" when applied to the protection of "official information." Executive Order 11652 uses the term "interest of the national defense or foreign relations of the United States (hereinafter collectively termed 'national security')" when applied to the protection of "official information." Repeated efforts were made during the hearings to clarify the reason for the change in terminology in the new order. No real explanation was provided by administration witnesses who testified.

The term "national security" had been used in Executive Order 10290, but had been replaced by "national defense" when President Eisenhower issued Executive Order 10501 in 1953. It also raised the issue of conflict with the language in the Freedom of Information Act (section 552(b)(1)), which permits the exemption of information "specifically required by Executive order to be kept secret in the interest of the national defense or foreign policy." [164]

[161] Ibid., see pp. 2694 et seq. for discussion and colloquy with Mr. Maroney on the subject of his speech; the text is on pp. 2711–2714.
[162] Ibid., p. 2695.
[163] Ibid., p. 2704.
[164] Ibid., pp. 2852–2853.

In addition to putting the language of the new Executive order at variance with the language of the Freedom of Information Act on which it relies for application of the exemption, the semantic and legal differences between the terms "national defense" and "national security" and the terms "foreign policy" and "foreign relations" weaken the entire foundation of Executive Order 11652, while failing to correct a basic defect in Executive Order 10501—namely, its lack of a definition for the term "national defense." For example, "relations" is a much broader word than "policy" because it includes all operational matters, no matter how insignificant.

The following colloquies involving Subcommittee Chairman Moorhead, Congressman Moss, Mr. Buzhardt (Defense), and Mr. Blair (State) illustrate efforts made during the hearings to obtain an explanation of the rationale behind the change in language in Executive Order 11652:[165]

> Mr. MOORHEAD. Mr. Buzhardt, one of the things that perturbs me about the new Executive order is its inconsistent language. While it does cite the Freedom of Information Act which does have the exemption (b)(1) that act uses the terms "national defense or foreign policy." However, the Executive order, although citing the act does not use that language which has been relied upon by the courts, which has been construed by the Attorney General, and which has been in use for now almost 5 years. It uses a different term, "national security," and then instead of using the words "foreign policy," it uses the words "foreign relations."
>
> At one point in your testimony, I think page 4, you said the category is broader. It seems to me that it would have been logical to use the statutory language which has been defined and not use another term which is broader, as your own testimony indicates, than the statutory language of the act.
>
> Mr. BUZHARDT. Let me say first that the term "national defense," as used in Executive Order 10501, has been generally construed by the courts and certainly interpreted by both the executive, well, certainly the executive branch, to include foreign relations matters. Now there is a possible slight distinction between foreign policy on the one hand and foreign relations on the other.
>
> We believe that foreign relations is a more precise term, and I will defer to Mr. Blair on this.
>
> Mr. MOORHEAD. You go back to Executive Order 10501. I was referring to the Freedom of Information Act. If there is a difference in meaning and if foreign relations are broader, then under the law passed by the Congress and signed by the President you can't expand that by using broader language.
>
> Mr. BLAIR. May I comment on that, Mr. Chairman?
>
> Mr. MOORHEAD. Yes.
>
> Mr. BLAIR. First, I would say that I think we tend to regard the distinction between the word "policy" in this context and the word "relations" as being rather minor, but of the two words we would regard relations as being more

[165] Ibid., pp. 2468–2471.

concrete. A question would arise in some cases if the word for this purpose were policy, in a case like this, where a telegram comes in from the field and the reason that it is being classified by the originating Ambassador or his staff is that it reflects, let's say invidiously on the head of state of a foreign government, and that, we feel, would damage our negotiations with that government now in progress if it were prematurely published. Well, is that a policy matter? That would be a question in some minds, an ambiguity; but we felt if you use the word "relations" it makes it quite clear that the President is instructing us or giving us authority to use our discretion to classify in such a case. Whether that is foreign policy or not I am not sure. * * *

* * * * *

Mr. Moss. First of all, I think we should have the record very clearly reflect that no authority is given the Executive to classify under the Freedom of Information Act, nor is any authority implied, but there is a recognition of an exemption for those items specifically, and the term "specifically" was used advisedly—specifically ordered to be protected by an Executive order.

So there is no expansion of whatever claim of Executive power the President might make based on our statutes. We had not intended and I think we were very cautious in not expanding by implication or otherwise any claimed authority of the President. We used the term, "defense and foreign policy" very carefully. We did not intend to cover foreign relations. It was proposed but we did not use that term at all because we felt that the foreign relations might be far broader than foreign policy. We do have a foreign policy that is set forth with some degree of clarity, varying from time to time by the Executive, and it is the text of that policy which concerned the committee in drafting the language.

Foreign relations go far beyond the policies which we might lay out, isn't that true?

Mr. BLAIR. I don't think in practice, Mr. Moss, that we have so interpreted it, but as I say, there has been the feeling that some ambiguity could arise under the other phrase.

Mr. Moss. You would not say that in drawing a definition for foreign policy and for foreign relations you would come up with the same definition, would you?

Mr. BLAIR. I would be hard put to come up with a very precise definition for either.

Mr. Moss. Couldn't you have foreign relations that occurred on a day-to-day basis that completely contravened the foreign policy of the United States?

Mr. BLAIR. I can only say that in practice we have understood both to be rather broad terms, Congressman Moss.

Mr. Moss. We used not foreign relations, we used foreign policy. We had the option of including foreign relations and we also had the option of dealing with national security. We

also rejected that as being far more comprehensive than we intended it to be in the act. National defense, rather specific; foreign policy, rather specific. We did not intend either foreign relations nor national security.

But in view of the fact you have moved to national security, can either of you gentlemen give me a definition of "national security"? And while you are at it, can you deal with a hypothesis of any instance where you could not reasonably, let's say, be expected to cause danger to national security?

It is very easy to construct a reasonable case of possible danger if a person would accept all of the elements of a hypothesis affecting that, isn't it?

Mr. BUZHARDT. Mr. Chairman, I think the test of reasonableness in this case is one that was imposed which did not exist under 10501. There it was any potential. The word used is "could."

Mr. Moss. 10501 used "might gravely impair or"——

Mr. BUZHARDT. Yes, that is a degree of danger.

Mr. Moss. Yes.

Mr. BUZHARDT. But the condition was established by the word "could." That is the word that was replaced by "reasonably expected to."

Mr. Moss. A test of reasonableness means that a reasonable man could be persuaded, and I say that taking the case of national security, such an ill-defined phrase, that no one can give you a definition. You can't. I invite you to do it on the record if you can. In 16 years of chairing the committee prior to Mr. Moorhead I could never find anyone who could give me a definition. But if you can I would be most interested in hearing it. * * *

Written responses were supplied for the hearing record by both the State and Defense Departments on this subject in an effort to further clarify the issue. The State Department response to the subcommittee's written question was as follows:[166]

Question 1. The new Executive order states that foreign relations information which is classified is expressly exempted from public disclosure by the Freedom of Information Act. In my view (Chairman Moorhead), that is not correct. Only foreign policy information which is classified is exempted from public disclosure but even that exemption is permissive and not mandatory. Foreign relations covers the waterfront. Foreign policy is much more specific—it deals only with policy and not the complete spectrum of all activities and operations. Foreign policy is a definite course of action adopted and pursued. Foreign relations is anything connected or associated with foreign policy. The new Executive order cited the Freedom of Information Act as one of its statutory authorities. But in actuality the Freedom of Information Act only recognizes the existence of a previous Executive order. It in no way authorizes such an order. Nor does the new order in any way change the meaning of the Freedom of Information Act. Do you have any comment on this overall observation?

[166] Ibid., p. 2516.

Answer. We recognize fully that no Executive order can change the meaning or intent of legislation. We believe the intent of Executive Order 10501, the Freedom of Information Act, and Executive Order 11652 in this context is identical in each case: to recognize and meet the need for temporary confidentiality for some information developed in the course of our diplomacy, the premature release of which would be likely to damage, in the words of the act, our "national defense or foreign policy" interests. The fact that the drafters of these various documents did not choose identical language has no bearing on the effect of the act; and we expect and intend that implementation of the new order shall limit, rather than expand, the amount, degree, and duration of future classification in comparison with previous practice, as the President in issuing the order has explicitly directed.

The answer for the record supplied by Mr. Buzhardt of the Defense epartment in response to Congressman Moss' request was:[167]

As used in Executive Order 11652, the term "national security" is explicitly used in a collective sense to encompass "national defense" and "foreign relations." (See sec. 1.) In my personal opinion, "national security," as used in this context, is synonymous with the generally understood definition of "national defense" as used in Executive Order 10501. In this context, "national security" is a generic concept of broad connotations referring to the Military Establishment and the related activities of national preparedness including those diplomatic and international political activities which are related to the discussion, avoidance or peaceful resolution of potential or existing international differences which could otherwise generate a military threat to the United States or its mutual security arrangements.

The term, although not specifically defined by statute, appears more than 164 times in the United States Code, 1964 edition, supplement V, based upon the research report produced by the LITE computer system, a copy of which is attached. The frequency of its use in Federal legislation suggests that it is a well understood term, and one readily accepted by the Congress. For example, Public Law 92–68, enacted August 6, 1971 (42 U.S.C. 2476) provides for annual reports to Congress on aeronautics and space activities, but excludes classified information, subsection (c) provides, "No information which has been classified for reasons of national security shall be included in any report made under this section, unless such information has been declassified by, or pursuant to authorization given by, the President." (Emphasis added.)

It is significant that although Executive Order 10501 used the term "national defense," the Congress chose to use the words "national security" in describing classified information.

[167] Ibid., p. 2470.

Later in the hearings, Assistant Attorney General Erickson was also asked to comment on this same issue: [168]

> Mr. MOORHEAD. Mr. Erickson, we have been endeavoring in this series of hearings to find out what was behind the change in the terminology from the old Executive order to the new Executive order, particularly the words "national security," which described as "national defense or foreign relations of the United States." Exemption (b)(1) of the Freedom of Information Act refers to "matters under Executive order required to be kept secret in the interest of national defense or foreign policy." It seems to us that the words "national security" are broader than "national defense." What you may have done is inadvertently taken yourself out from under the exemption language in section (b)(1) of the act.
>
> Can you explain the rationale behind the change to "national security" from "national defense and foreign policy"?
>
> Mr. ERICKSON. Mr. Chairman, I was not personally involved in the development of this definition. I do know, however, that the insertion of the definition for national security was placed there principally for the purposes of clarification, in the sense that the use of the term national defense in Executive Order 10501 has rather consistently been interpreted within the executive branch to include matters of foreign relations. It was not the intent, in establishing the definition of national security, to expand the scope of the material covered by Executive Order 11652.

It was also pointed out in a colloquy with Mr. Erickson that the report of the National Commission on the Reform of the Federal Criminal Laws, also called the Brown Commission, recommending revisions in the Federal Criminal Code had suggested the use of the term "national security information" in references to the Espionage Act, contained in title 18 of the United States Code. The witnesses were asked if the reason why the term "national security" was substituted for "national defense" in section 1 of Executive Order 11652 might not be that the administration wished to conform the language of the Executive order to this language contained in the Brown Commission's recommendations. Mr. Erickson stated "that aspect has not been considered by the department yet, to my knowledge, and certainly is not the basis for national security as it appears in the Executive order." [169]

It would thus appear that the question of terminology discussed above has not been resolved, although the detailed discussion of the question during the hearings helped focus attention on the broad dimension of the problem.

Number of Persons Authorized To Classify

Another of the major questions discussed during the hearings was the wording of section 2 of Executive Order 11652—"Authority to Classify"—concerning the potential "trickle-down" spreading of

[168] Ibid., p. 2688.
[169] Ibid., pp. 2704–2705.

classification authority without limitation of the numbers of persons authorized to wield classification stamps, despite a requirement of the order that delegation of authority must be in writing.[170]

Executive branch witnesses assured the subcommittee during the hearings that the numbers of persons authorized to classify "Top Secret," "Secret," and "Confidential" under the new order would be vastly reduced in their own departments and from an overall standpoint. As has been noted earlier at page 40 of this report, Ambassador John Eisenhower, Chairman of the Interagency Classification Review Committee indicated in an August 3, 1972, release that the overall reduction of persons authorized to classify under Executive Order 11652 has been some 63 percent in major departments.

The committee is gratified with this apparent downward trend, but reiterates that a reduction in the numbers of persons authorized to classify does not, in itself, resolve the problem of excessive classification and the continued proliferation of the volume of documents classified. Moreover, the committee has not itself confirmed the accuracy of these figures.

No Specific Penalties for Overclassification

Another defect examined during the hearings was the failure to include specific sanctions in Executive Order 11652 against unnecessary classification or overclassification.[171] Both the old and new orders warn against such actions, but it has been painfully clear to this committee that such has not done much good in the past.

As noted earlier in this report, this committee has for many years strongly condemned overclassification of documents under Executive Order 10501 and its implementing directives and regulations and recommended full enforcement, including disciplinary action, of provisions of the order prohibiting such overclassification.[172]

But, despite these efforts there has been little real movement by the executive branch toward this objective. Former Defense Secretary McNamara's 1961 admonition "* * * When in doubt, underclassify," did little, if anything, to curb excessive classification in that department, even though Defense Department witnesses acknowledged during the 1971 hearings that the McNamara directive was still in effect.[173]

As part of the subcommittee's January 1972 questionnaire to selected executive departments and agencies having major responsibilities for security classification matters, statistical data was solicited concerning formal investigations between July 1, 1967, and June 30, 1971, into possible violations of regulations governing the protection of information classified under Executive Order 10501. Detailed questions dealt with investigations concerning improper physical protection of information, with failure to designate a high enough security

[170] Ibid., pp. 2854-2856.
[171] Ibid, p. 2858.
[172] See p. 23 of this report.
[173] Hearings, pt. 2, p. 683.

designation, and with the assignment of too high a security designation. Other information requested concerned criminal charges filed as a result of these investigations, administrative hearings held, and administrative penalties assessed.[174]

The analysis of responses to the questionnaire showed that during this 4-year period, these agencies carried out 2,433 investigations of violations of regulations governing the classification of information under Executive Order 10501. They assessed administrative penalties, ranging from reprimands to loss of pay, against 2,504 individuals involved in the investigations. But only two of the investigations involved cases of overclassification and not a single administrative penalty was imposed against overclassification.[175]

This failure to apply sanctions against overclassification—one of the most obvious shortcomings of Executive Order 10501 and one of the basic reasons for its replacement by the new order—was a reluctance to implement the intent of section 3 of Executive Order 10501, which clearly specifies that "Unnecessary classification and overclassification shall be scrupulously avoided." [176]

Executive Order 11652 used virtually identical language in section 4 to warn against such practices—"Both unnecessary classification and overclassification shall be avoided." The new order does add two additional sentences to reinforce the prohibition which, hopefully, will be taken more seriously by Government classification officials who wield the secrecy stamps in executive agencies: [177]

> Classification shall be solely on the basis of national security considerations. In no case shall information be classified in order to conceal inefficiency or administrative error, to prevent embarrassment to a person or Department, to restrain competition or independent initiative, or to prevent for any other reason the release of information which does not require protection in the interest of national security.

Section 13(A) of the new order also contains another salutary provision:

> Any officer or employee of the United States who unnecessarily classifies or overclassifies information or material shall be notified that his actions are in violation of the terms of this order or a directive of the President issued through the National Security Council. Repeated abuse of classification process shall be grounds for an administrative reprimand. In any case where the Departmental committee or the Interagency Classification Review Committee finds that unnecessary classification or overclassification has occurred, it shall make a report to the head of the Department concerned in order that corrective steps may be taken.

It is obvious that only by the full and vigorous enforcement of the necessary implementing regulations by all executive agencies exercising classification authority under Executive Order 11652 can there be

[174] See hearings, pt. 2, p. 2931 for text of questionnaire; also pp. 2929–2937 for memorandum from Congressional Research Service, Library of Congress analyzing the responses from executive agencies; a summary table may be found at pp. 2935–2937; the texts of agency responses are at pp. 2723–2820.
[175] Hearings, pt. 7, table at pp. 2935–2937.
[176] Ibid, p. 2858.
[177] Ibid.

effective administration of the security classification system to prevent the unnecessary classification and overclassification that undermined the effectiveness of the old order.

It is significant to note that of the implementing regulations issued thus far, only the State and Justice Departments contain positive language in their administrative penalty sections that specifically mentions "overclassification" within the application of the sanctions. The Defense Department language on administrative actions merely applies such penalties to those officers or employees guilty of "repeated abuse, repeated failure, neglect, or disregard of established requirements with respect to safeguarding classified information or material * * *," as provided in section 13(A) of the Executive order. But there is no specific mandate against "overclassification" in the DOD implementation directive, the one executive department where the bulk of the overclassification abuses under Executive Order 10501 had occurred.[178]

Identity of Classifiers and Accelerated Declassification

Two other shortcomings in Executive Order 11652 dealt with Section 4(B)—"Identification of Classifying Authority"—and Section 5—"Declassification and Downgrading."[179]

The committee has noted in past studies of the security classification system that the failure to require that classified documents be identified with the name of the official exercising classification judgment authority was a basic weakness in Executive Order 10501. The language of section 4(B) of Executive Order 11652 is a step forward in that it provides that "material classified under this order shall indicate on its face the identity of the highest authority authorizing the classification." This language is somewhat diluted, however, by the beginning phrase of the section which qualifies this requirement by stating: "Unless the Department involved shall have provided some other method of identifying the individual at the highest level that authorized classification in each case. * * *" Thus, a "code" system of identification is permitted.

Subsequent staff analysis of implementing directives and regulations indicate that, generally, they require that the classifier be clearly identified on the face of the document. The Justice Department regulations do permit "code" identification of classifiers in cases where the identification by name "might disclose sensitive intelligence information."[180]

Additional concern was expressed over language of section 5 of the new order, dealing with declassification and downgrading procedures. It was based on the failure to include language contained in section 4 of Executive Order 10501, which provided for the downgrading or declassification of classified information when it "no longer requires its present level of protection in the defense interest." The new order contains no requirement to depart from the rules of the general declassification schedule.

[178] 37 F.R. 15644 (state—Sec. 9.64, title 22, CFR); 37 F.R. 15646 (Justice—sec. 17.7, title 28, CFR); 37 F.R. 15679 (Defense—sec. 159.1400, pt. 159 to DOD Directive 5299.1, "DOD Information Security Program").
[179] Ibid., pp. 2859–2860.
[180] 37 F.R. 15648 (sec. 17.21, title 28, CFR).

The committee notes that the National Security Council directive, issued on May 19, 1972, does indeed correct this earlier omission in the language of Executive Order 11652. The first sentence of the section of the directive dealing with downgrading and declassification reads:[181]

> Classified information and material shall be declassified as soon as there are no longer any grounds for continued classification within the classification category definitions set forth in Section 1 of the Order. * * *

The new Defense Department Directive (pt. 159 to DOD Directive 5200.1), also contains a clear statement of such policy:[182]

> * * * When classified information is determined in the interests of national security to require a different level of protection than that presently assigned, or no longer to require any such protection, it shall be regraded or declassified."

Extending the Secrecy Barrier

Another major concern over the shortcomings of Executive Order 11652 involved the 10-year general declassification schedule provided for in section 5 of the order.[183] Under Executive Order 10501, certain nonexempt categories of classified information were downgraded at 3-year intervals from the 12-year starting point. Executive Order 11652 provides that "Top Secret" information becomes "Secret" at the end of the second full calendar year following the year in which it was originated. It then becomes "Confidential" at the end of the fourth full calendar year following the year in which it was originated and is declassified (unless it falls into one of the four exempt categories) at the end of the tenth full calendar year following the year in which it was originated.

Section 5(B) of Executive Order 11652 describes the four categories of information that may be exempted from the general declassification schedule:[184]

> (1) Classified information or material furnished by foreign governments or international organizations and held by the United States on the understanding that it be kept in confidence.
>
> (2) Classified information or material specifically covered by statute, or pertaining to cryptography, or disclosing intelligence sources or methods.
>
> (3) Classified information or material disclosing a system, plan, installation, project or specific foreign relations matter the continuing protection of which is essential to the national security.
>
> (4) Classified information or material the disclosure of which would place a person in immediate jeopardy.

The positive results of the reduction of the declassification schedule from 12 years under the old order to 10 years under Executive Order 11652 may, however, be more illusory than real. The classification

[181] 37 F.R. 10054; see text in hearings, pt. 7, p. 2320.
[182] 37 F.R. 15658 (sec. 159.103-1); see also hearings, pt. 7, p. 2361.
[183] Hearings, pt. 7, pp. 2860-2862.
[184] Ibid., pp. 2861-2862.

category downgrading of section 5(B) provides that such action be taken "at the end" of the various applicable calendar years "following the year in which it was originated." For example, a document classified top secret early in 1973 would not be downgraded to secret until Decembr 31, 1975—or almost 3 years later, not the 2-year period indicated at first glance. This same document would not be downgraded to confidential until December 31, 1977, and, assuming it was not a matter falling into the exemption categories of section 5(B), it would not be declassified until December 31, 1983. This is a period of 10 years—plus another period of up to 12 months, depending upon how early in the applicable classification year the document was originally classified.

The potential for political abuse of the provisions of section 5 of the new order is also of major concern to the committee. The continued classification of vital information concerning key national defense and foreign policy issues for a period of 10-plus years under the general downgrading and declassification schedule means that any President could complete his two constitutional 4-year terms in office without having to account to the electorate for major policy blunders in these areas that might have taken place. Moreover, it would be possible for his Vice President or other nominee of his political party to succeed him without the public knowing full details of these defense or foreign policy errors committed by the administration and hidden away under the classification stamp.

The potential abuse of this section of the new order is compounded by the language of section 5(B), providing broad exemptions to the general downgrading and declassification schedule. For example, the language of exemption (3) dealing with classified information dealing with a "specific foreign relations matter" means that major policy errors of potential embarrassment to an administration in power could be withheld from the American public for periods far in excess of the 10-plus-year period—up to 30 years or longer under provisions of section 5(E).

These serious and politically sensitive issues, raised during the hearings, remain matters of continuing concern to the committee. They raise questions of potential abuses, regardless of which political party may occupy the White House.

Need for Adequate Oversight by Congress

The lack of cooperation by Executive Office personnel with the subcommittee regarding the draft of the new Executive order and their refusal to testify on technical details of the order prompted efforts by Members during the hearings to determine from other executive branch witnesses the degree of oversight which this committee and other committees of the Congress will be able to exercise over the operation of the classification system under Executive Order 11652.

Part of this concern stems from the fact that section 7 of Executive Order 11652—"Implementation and Review Responsibilities"—provides that "The National Security Council shall monitor the implementation of this order." It also provides for the establishment

of an Interagency Classification Review Committee (ICRC) to assist the NSC in this regard, composed of representatives of the Departments of State, Defense, and Justice, the Atomic Energy Commission, the Central Intelligence Agency, the National Security Council staff, and a chairman designated by the President.[185]

While sections 13, 17, and 18 of Executive Order 10501 provided for broad review and implementation responsibilities under the NSC, within each department, and by a White House staff designee, the lack of vigorous enforcement and implementation was a root cause of the breakdown in the security classification system under the old order. The newly created ICRC is an effort to help remedy this crucial weakness in the system. In his statement accompanying the new order, President Nixon said:[186]

> Of critical importance to the effectiveness of my Executive order will be the new administrative machinery designed to ensure that its provisions are not allowed to become mere meaningless exhortations. The National Security Council will monitor compliance with the Executive order. In addition, the order creates a small Interagency Classification Review Committee with extensive powers to oversee agency implementation of the new system, and to take action on complaints both from within and from outside the Government on the administration of the order.

Nothing is said about the accountability of either these two groups to committees of Congress. But the record of immunity of the national security staff to congressional oversight raises questions about the possible use of "executive privilege" to afford sanctuary to officials involved in key administrative supervisory roles under the new order.

Several efforts were made during the hearings and in subsequent written questions to executive branch witnesses to establish the degree to which the activities of the ICRC would be subject to congressional oversight. The following exchanges with Defense Department General Counsel Buzhardt and with then Assistant Attorney General Erickson illustrate the problem:

> Mr. MOORHEAD. Mr. Buzhardt, you discussed the role of the Interagency Classification Review Committee. I gather that this would be under the National Security Council?
>
> Mr. BUZHARDT. Yes, Mr. Chairman.
>
> Mr. MOORHEAD. What I want to know is how can the Congress of the United States exercise its oversight responsibility over the actions of the Classification Review Board. How can we? Who can we have testify? Will there be someone designated to represent that committee before the committees of Congress?
>
> Mr. BUZHARDT. Mr. Chairman, I don't know what the National Security Council directive will say or will not say on this point but I will say that if the departments have representation on it, we in the departments will be subject to your oversight and your pressure for hearings and this sort of thing.[187]

* * * * *

[185] Ibid., pp. 2876–2877. See also footnote 113, p. 40 of this report.
[186] Ibid., p. 2312.
[187] Ibid., pp. 2475–2476.

Mr. MOORHEAD. Let me ask you this, Mr. Erickson—if this subcommittee, in its oversight over the Freedom of Information Act or some other appropriate committee of the Congress, wanted to check up on the administration of the new Executive order, who would we ask to come before us as a witness to explain what has been done, who from the National Security Council?

Mr. ERICKSON. I would expect that those who assist you in your oversight function would be representatives from the various departments, particularly those involved with or participating on the Interagency Review Committee. I would not expect that it would be anyone in particular from the National Security Council.

Mr. MOORHEAD. Will there be a chairman of the Interagency Committee?

Mr. ERICKSON. Yes; there will be a chairman.

Mr. MOORHEAD. And from what agency will he come?

Mr. ERICKSON. I do not know. A chairman, as I believe you know, has not been selected.

Mr. MOORHEAD. But will he be available to committees of the Congress so that we can monitor and assist the Interagency Committee?

Mr. ERICKSON. Until I know who the chairman is I can't realistically answer that question.

Mr. MOORHEAD. Are you suggesting that if he comes from the National Security Council he would not be available for congressional inquiry?

Mr. ERICKSON. I think that is a question that would have to be answered on a case-by-case basis. I could not state categorically at this time whether he would or would not be available.

Mr. MOORHEAD. I think for the good of the nations that an arrangement should be made so that the Congress can have a way to determine whether or not the excellent statement of the President saying that we are going to have a more "open government" is really being carried out. I think this is important to restore confidence in government. Whatever input you can give to that principle would be of great service.[188]

Several written questions were also directed to the State, Defense, and Justice Departments in an effort to obtain a clearcut answer to the basic question of congressional oversight. The questions and responses from the State Department were as follows:[189]

Question 4. What role will Congress play in monitoring the new Executive order? Is the interagency review committee you described in your statement answerable to Congress? If not, why isn't it? It claims statutory authority from Congress.

Answer. Congress should be able to monitor the implementation of the new Executive order more effectively than in the case of the old order, in view of the concentration of responsibility for the diverse functions involved in a single principal

[188] Ibid., pp. 2685–2686.
[189] Ibid., pp. 2516–2517.

officer of each agency concerned. In our judgment, the Interagency Classification Review Committee, like other committees of the National Security Council, will not be answerable to Congress in a legal sense, but the departments and agencies represented on it, and their representatives, of course will continue to respond to congressional oversight.

Question 9. National Security Council policies, practices, and procedures are exempt from disclosure to the Congress or the public under existing Presidential directive. By placing the overview of Executive Order 11652 under the NSC, will not this shield such supervisory functions from congressional and public scrutiny?

Answer. See reply to question 4. More broadly, while we cannot speak for the committee, which will be holding its first meeting shortly, we would anticipate that the committee like its member agencies will be sensitive to congressional and public interest in its performance and will do its best to see that both are kept well informed.

Responses from the Defense and Justice Departments were equally vague and disconcerting:

Question 9. Mr. Buzhardt, you discuss the role of the Interagency Classification Review Committee on page 10 of your statement. Of course, as written, it is under the National Security Council. How is Congress going to be able to effectively exercise its oversight responsibility in such a situation when we can't even get the draftsman of the order to come before us to help explain its provisions and rationale? Will the chairman be designated to be the spokesman for the committee in testimony before congressional committees? If not, who will testify?

Answer. I am confident that the executive branch will find a means of providing the necessary information needed in the performance of its oversight responsibilities.

Question 19. National Security Council policies, practices, and procedures are exempt from disclosure to the Congress or the public under existing Presidential directive. By placing the overview of Executive Order 11652 under the NSC, will not this shield such supervisory functions from congressional and public scrutiny?

Answer. I do not believe it appropriate for me to speak for the National Security Council.[190]

* * * * *

The Justice Department responded as follows:

Question 7. Since the present Administration prohibits the disclosure of all information generated by or under the direction of the National Security Council on the basis of "executive privilege," will not Congress and the public be unable to find out whether the NSC is carrying out its responsibilities under Executive Order 11652 regarding the administration of the Order and implementation and review under it?

Answer 7. As you know, the decision whether to invoke Executive privilege with respect to information requested by

[190] Ibid., p. 2521 and p. 2523.

> Congress is made only by the President. The decisions whether to invoke it are made on a case-by-case basis, after a specific request has been made. We are not in a position to predict what the President's decision will be in regard to future requests.[191]

While individual departmental or agency members of the ICRC may be willing to testify before committees, the question remains unanswered as to whether or not the Chairman or other spokesmen for the ICRC as an entity will be permitted by the President to appear at oversight hearings. This is a matter of deep concern to the committee and its implications should also be obvious to all Members of Congress.

Use of Access, Distribution, or Control Markings

The hearings also probed into another area of concern over the language of section 9 of Executive Order 11652—"Special Departmental Arrangements"—that governs the use of special access, distribution or control markings on classified information.

One of the difficult problems related to the effective operation of the security classification system has been the widespread use of dozens of special access, distribution, or control labels, stamps, or markings on both classified and unclassified documents. Such control markings were not specifically authorized in Executive Order 10501, but have been utilized for many years by many executive agencies having classification authority and dozens of other agencies who do not possess such authority.[192] The use of such stamps has, in effect, been legitimized in section 9 of the new Executive Order 11652.

Among agencies having classification authority under Executive Order 10501, those that utilized such control labels averaged 5 per agency. The Defense Department listed some 13 labels, such as "SIOP," "SPECAT," "NOFORN," and "Proprietary."[193] Authority to use such labels or markings is often vague; some agencies cite no authority, while others rely on instructions contained in manuals, handbooks, directives, or administrative regulations. A few agencies cite statutory authority such as the Atomic Energy Commission, the Defense Department, and the Arms Control and Disarmament Agency. In all, more than 60 such control markings or labels were identified as a result of the subcommittee's questionnaire to executive agencies.

The Treasury Department, in its response to the questionnaire, indicated that they did not use any such labels. Yet in subsequent testimony, the Internal Revenue Service admitted that they applied such labels as "For Official Use Only," "Limited Official Use," and "For National Office Official Use Only."[194]

The rationale behind the use of such markings was discussed in several colloquies during the hearings with State and Defense Department officials:[195]

[191] Ibid., pp. 2823–2824.
[192] See hearings, pt. 7, pp. 2929–2934 for analysis of responses to an August 1971 subcommittee questionnaire to executive agencies, prepared by the Congressional Research Service, Library of Congress; see also pp. 2723–2820 for text of agency responses to the subcommittee questionnaire.
[193] Ibid., pp. 2495–2496; pp. 2728–2729; also hearings, pt. 2, pp. 665–666.
[194] Ibid., pp. 2931–2932 and hearings, pt. 6, p. 1990; pp. 2027–2030.
[195] Hearings, pt. 7, pp. 2477–2479; also pp. 2493–2499.

Mr. MOORHEAD. Mr. Blair, in responding to the subcommittee's questionnaire the Department listed several authorized "channel captions". How do these authorized channel captions control information? What authority is there for the use and do they really in effect serve as classification devices?

Mr. BLAIR. Well, they are not classification devices, Mr. Chairman, they are internal government distribution controls which attempt to enforce the need-to-know principle. That is to say that just because I am authorized to receive a top secret document it doesn't mean that I should thereby see every top secret document. I should only see those which relate to those things which I am responsible for. So that a given top secret document coming in from the field may be, not always, but may be marked with one of these controls that you mentioned, one of these captions which indicates which people within the Department of State or, perhaps within the family of agencies are entitled to receive information on that particular subject.

So far as availability of the document to the public is concerned, it has no bearing whatsoever. The classification, of course, would govern.

Mr. Blair, Deputy Assistant Secretary of State for Public Affairs, further stated:

Mr. BLAIR. * * * We are narrowing them down from the standpoint of distribution of documents within the Government to those people who have responsibility for the subject matter concerned. But if a question came in under the Freedom of Information Act or from the Congress or other representative of the public for that given document, the fact that it is marked, let's say, NODIS, is not relevant. What is relevant to the making available of that document to the public is whether or not it was properly classified under the Executive order and whether or not the Freedom of Information Act, for example, once we have reviewed the document, still pertains, whether we feel that the need for the classification still pertains and whether, in fact, we are authorized under the act to hold it. * * *

During this same colloquy, the Defense Department's General Counsel, Mr. J. Fred Buzhardt, commented: [196]

Mr. BUZHARDT. * * * We are talking about two entirely different things. If we start with classified documents, those documents are not to be revealed to unauthorized persons.

With respect to classified information, there are two requirements for access, one of which is that the individual must have clearance, that means that there has been a prior determination that the individual is trustworthy. The second requirement is that he has a need to know in his official capacity to use the information. Once the determination is made that information must be protected, one of the devices used to protect it is not to disseminate it beyond those who

[196] Ibid., p. 2479.

> have some official reason or a business reason to use the information. Obviously the more narrow the distribution, the easier it is to protect the information from unauthorized disclosure.
>
> As a consequence, access limitations are imposed, sometimes by marking on the document, sometimes because the man doesn't show it to his subordinates, for instance, he makes a judgment they do not need to see it. * * *

The question was raised as to the effect of the legitimization of the more than 60 access or control stamps or labels and whether or not such proliferation of internal agency stamps would not make it more difficult to afford maximum security protection to truly important classified documents. Mr. Buzhardt was asked his opinion on this question concerning section 9 of the new Executive order and whether or not it runs counter to one of the major objectives of the order—to reduce the volume of classified material. He replied: [197]

> Mr. BUZHARDT. No, it is not. In the first place, you have a determination as to whether the material is to be classified. Once the decision is made that the information should be classified, then the limitation of access has to do with the protection of that which is classified. We also have the responsibility to control the dissemination. That is what these access limitations are for, to control dissemination, to confine access to the people who have a need to know to work with the information. It is a protection device. We must use protective devices of some sort. We lock them in safes, you prevent people who don't need to see them from seeing them. But the original decision is whether it should be classified. * * *

Mr. Blair added:

> Mr. BLAIR. * * * The purpose of classification is to determine what information is or is not available to the public outside of the government. These labels that you are referring to have nothing to do with that. They have absolutely no value for determining what information or what document may be given to a member of the public. They are simply a mailing device, if you like, a means by which a superior determines which of his subordinates he wishes to deal with this particular matter and be aware of this particular information. * * *

The National Security Council's directive implementing Executive Order 11652, issued several weeks later, provides extensive guidelines on marking and access requirements. In its brief reference to section 9 of the order, the NSC directive states:[198]

> F. Restraint on Special Access Requirements.—The establishment of special rules limiting access to, distribution and protection of classified information and material under section 9 of the order requires that specific prior approval of the head of a department or his designee.

[197] Ibid., p. 2497.
[198] Ibid., pp. 2322–2325.

Special access regulations issued by departments in August 1972 to implement section 9 requirements and those of the NSC directive follow the general "need to know" criteria.[199]

Thus, while there is a clear rationale for the use of such access or control markings, the basic problem is the effect of the proliferation of their use on the effective operation of the classification system. This problem, fully explored with executive branch witnesses during the hearings, is one that this committee believes should be carefully monitored by the Interagency Classification Review Committee and by departmental heads to assure that it does not interfere with the overall effectiveness and integrity of the classification system.

Mandatory Review of Exempted Material

The final major area of criticism directed at Executive Order 11652 that was discussed during the hearings involved the "Mandatory Review of Exempted Material" after the 10-year classification period, as provided for in section 5(C). This provision and that contained in section 5(E), providing for the declassification of all classified information or material 30 years or older, have been highlighted as significant forward steps in the new order.[200]

Section 5(C) applies to the four categories of exempt information described earlier at page 70 of this report, and represents the most sensitive categories of information, the disclosure of which would be the subject of public interest. Examples might be documents relating to the abortive Bay of Pigs expedition in 1961, the Cuban missile crisis in 1962, and the Gulf of Tonkin incident in 1964. Of course, some information within each of these categories—such as that dealing with intelligence sources or that might place a person in jeopardy—would still be withheld under the exemption, even though many other documents related to such operations could be disclosed.

Executive Order 11652 provides for a "classification review by the originating department at any time after the expiration of ten years from the date of origin." [201] Three conditions are imposed—"(1) A department or member of the public requests a review; (2) The request describes the record with sufficient particularity to enable the Department to identify it; and (3) The record can be obtained with only a reasonable amount of effort." If the reviewing authority determines that the information or material no longer qualifies for exemption, it shall be declassified. If the reverse is the case, the information shall be so marked and unless impossible under the criteria, a date for automatic declassification is to be set.

One of the obvious problems that the requester for the mandatory review of certain classified information over 10 years old will encounter is that of identification of the information "with sufficient particularity to enable the Department to identify it." Another limiting provision of the Executive order is the requirement that it can be obtained with only a "reasonable amount of effort" on the part of the Department. The Department is, of course, the sole judge of the way in which these requirements are interpreted.

[199] See 37 F.R. 15631 (State—Sec. 9.20, title 22 CFR); 37 F.R. 15652 (Justice—Sec. 17.59 and 17.63, title 28, CFR); 37 F.R. 15678 (Defense—Sec. 159.1200, pt. 159 to DOD Directive 5200.1, "DOD Information Security Program").
[200] Ibid., pp. 2862-2864.
[201] Ibid., p. 2862.

The extent to which information subject to section 5(C) disclosure is actually made available to the public is one of the major criteria for judging the overall progress the new Executive order is making to carry out its announced principles to advance the public's right to know. The committee will carefully observe how such requests for mandatory review are handled and the types and volume of such information eventually made available to the public.

Historians and scholars have a special interest in the provisions of section 5(E) of Executive Order 11652 that provide for the automatic declassification of classified information 30 years or older. Such categories of records are to be reviewed for declassification by the Archivist of the United States. However, the head of the department originating the classification of any such information may determine in writing that it requires continued protection beyond the 30-year period.[202]

This "savings" provision may actually dilute the purpose of the section and mean that such information may thus be continued in its classified status for "an undetermined number of years."

Written questions submitted to DOD General Counsel Buzhardt were directed to other aspects of the "mandatory review" section of the new Executive order. Another question dealt with its relationship with the Freedom of Information Act. His responses to these two questions were:[203]

Question 3. At the bottom of page 2 of your statement, you discuss "mandatory review" procedures. I think the term is totally misleading because of the criteria applied to it. How could a citizen meet the criteria under Section 5(C) of the Executive order? How could he "describe the record with sufficient particularity to enable the Department to identify it?" Even if he could, what would prevent the Department from refusing to review its classification because only they would say what was "a reasonable amount of effort."

Answer: The phrase "mandatory review" is valid. My testimony reflects two explicit requirements of the Executive order. Mandatory review must result when these two requirements are met. Although these two requirements provide for some flexibility, they will be interpreted and applied within the Department of Defense with due regard to the overall intent of the Executive order to expedite declassification and make more information more readily available to the public. Department of Defense monitoring and enforcement activities will assure integrity of the operation.

* * * * *

Question 7. On page 9 of your statement you again discuss that misleading term "mandatory review," permissible after 10 years. Isn't it true, that, if a request were made for an identifiable document under the Freedom of Information Act, such a review would necessarily be made at any time after its classification date?

[202] Ibid., pp. 2863-2864.
[203] Ibid., p. 2520.

> Answer: The Freedom of Information Act does not expressly provide for a mandatory classification/declassification review of classified information. The Executive order, however, provides that after 10 years, the review of requested classified information is mandatory. The practice of the Department of Defense under the Freedom of Information Act, however, is that if a requested document is found to be one which is classified, the document will be reviewed for possible declassification before a decision is made on the request. While the Freedom of Information Act permits requests to be submitted at any time, it is reasonable to expect that the nearer in point of time to a classification determination that a request is made under the Freedom of Information Act, the more likely it is that the classification would be confirmed upon review.

Dr. James B. Rhoads, Archivist of the United States, described how, in his judgment, section 5(C) of the new order would affect his operations:[204]

> A second provision of the Executive order, which is also new, and which we believe will have far-reaching consequences is that in section 5(C) which provides for the "mandatory review of exempted material." Under the present system either researchers or we can request agencies to conduct a review of classified documents. But there is no way in which either of us can really compel such a review. The new Executive order will permit this to be done with regard to all records more than 10 years old. Those documents in our holdings which we, ourselves, acting under agency guidelines cannot declassify, can be sent to the agencies, who must act upon them and who must act with reasonable speed. We believe that this provision will lead to the opening of significant quantities even of fairly recent classified material.

Regulations were subsequently issued to carry out the role of the National Archives and Records Service in the handling of requests for mandatory review of classified information over 10 years old. A procedure has been established to obtain a determination within 30 calendar days on such requests.[205]

As in other specific examples of variation of opinion as to the effect or meaning of certain sections of Executive Order 11652 discussed above, the real impact of these provisions must await evaluation. The committee intends to continue its oversight into the operation of the "mandatory review" and "30-year automatic declassification" features along with the other major areas of contention connected with the new order.

Lag in Implementation of New Order

As was noted earlier at pages 55–56 of this report, there was a hiatus extending from June 1, 1972, until August 3, 1972—a period of some 64 days—between the effective date of Executive Order 11652 and the promulgation of regulations and directives by the six departments

[204] Ibid., p. 2606.
[205] Ibid., pp. 2394–2395.

and agencies most significantly affected by the new order. There was no "savings clause" in Executive Order 11652 to extend the provisions of the old order until such time as the NSC guideline directive and departmental and agency regulations had been issued, distributed, and taken full effect.

During the hearings, efforts were made to assess the progress being made some 2 months after issuance of the new order. As mentioned earlier, Subcommittee Chairman Moorhead had expressed concern that there would be sufficient time for proper implementation and had urged the President to suspend the effective date of the new order.[206] Executive branch witnesses were questioned on this point: [207]

> Mr. MOORHEAD. Mr. Buzhardt, you say that the Defense Department's implementation of the Executive order is dependent upon the National Security Council directive. Have you received that directive?
>
> Mr. BUZHARDT. No, we have not, Mr. Chairman.
>
> Mr. MOORHEAD. The implementation of the Executive order is dependent on a National Security Council directive which you haven't received and yet the Executive order is to take effect in less than 30 days.
>
> Mr. BUZHARDT. Yes, sir, Mr. Chairman, that is correct.
>
> Let me say that we haven't just sat back and waited. We have tried to anticipate, and we have done a lot of research and work identifying where people are that classify. We have reviewed the physical storage requirements. We have done a number of things so that we can have the information at hand hopefully to get our own regulations out promptly when the National Security Council directive is issued. But, of course, we cannot finalize anything until we do. We hope it comes out very shortly.
>
> Mr. MOORHEAD. What is the status, as you understand it, of the directive?
>
> Mr. BUZHARDT. I understand that is it being worked on, Mr. Chairman. I haven't been personally involved in it.
>
> Mr. MOORHEAD. Will there be time after you get the directive, even though you have done some anticipatory work, to get the implementation regulations out to the field, to carry on the training program to explain to the subordinates how they are to operate under this new Executive order?
>
> Mr. BUZHARDT. I think we will be able to get the regulations out, Mr. Chairman. I do not think obviously we will be able to conduct a training program before June 1. It will have to follow. And it will be undoubtedly a gradual process to make this thing effective. It is not going to be possible, we are moving as fast as possible, but I don't think it will be likely that we get 100-percent implementation right off the bat.

Another colloquy took place on this subject between Congressman Moss and the State and Defense Department witnesses: [208]

[206] See pp. 53–55 of this report.
[207] Hearings, pt. 7, p. 2480.
[208] Ibid., p. 2484. The State and Defense Departments regulations were actually issued on Aug. 3, 1972.

Mr. Moss. Over in State, Mr. Blair, who has been assigned the responsibility of implementing?

Mr. BLAIR. Sir, the prime responsibility in the stage in which we are now in, that is, for preparing the Department's regulations under the Executive order has been assigned to the head of the Office of Security, our Deputy Assistant Secretary for Security. Of course, I mentioned in my statement that we have a more broadly supervisory body in this area, newly established last year—the Council for Classification Policy; and the Council will be monitoring it in a policy sense.

Mr. Moss. But there has been a specific assignment?

Mr. BLAIR. Yes.

Mr. Moss. In the Department of State. And this is to the office of the Deputy Assistant Secretary for Security.

Mr. BLAIR. His responsibility at this stage is limited to drawing up our regulations.

Mr. Moss. To draft the regulations. Now who is that party?

Mr. BLAIR. By name? Marvin Gentile, Deputy Assistant Secretary for Security.

Mr. Moss. Now, is there any kind of a timetable available for completion of drafts, of implementing directives, by the departments?

Mr. BUZHARDT. No; there is not, Mr. Moss. We can't set a timetable on completing the drafts until we have the Executive order, I mean the National Security Council directive.

Mr. Moss. There is a timetable, is there not, implicit in the Executive order—June 1?

Mr. BUZHARDT. Yes, June 1 is to the effective date.

Mr. Moss. That is a timetable, isn't it? But between now and June 1 you have no timetable? You may come up to June 1 and what if you have no NSC directive at that point, do you fall behind?

Mr. BUZHARDT. I anticipate that we will have a National Security Council directive well before June, Mr. Moss.

Mr. Moss. With the care that the Pentagon puts into planning, don't you have an alternative plan in case you don't have the directive?

Mr. BUZHARDT. At the moment if it gets down to about 2 weeks, more, Mr. Moss, I assure you we will come up with one.

Assistant Attorney General Erickson also discussed the implementation status of the new order during his testimony:[209]

> Finally, I would like to comment generally on the procedures for the implementation of Executive Order 11652. As you know, the order contemplates the issuance of implementing directives through the National Security Council. The initial directive which I expect will be issued shortly will be a major step forward. While awaiting the issuance of that directive, affected agencies have been taking steps toward

[209] Ibid., p. 2680.

establishing their own procedures under the order: after the directive has been issued they can move forward rapidly in fulfilling their obligations under section 7 of the order. We remain hopeful that the administrative and operational aspects of the new security classification system will be in order by June 1 of this year.

Some idea of the confusion that existed during the 64-day hiatus on matters involving classification can be obtained by an example involving the State Department which came to the subcommittee's attention. During this interim period after the effective date of the new order and the promulgation of departmental regulations, the subcommittee received classified documents from the Department's Washington headquarters, which utilized the new classification procedures of Executive Order 11652. This was approximately 5 weeks prior to the issuance of the State Department's regulations. About the same time, the subcommittee also received a document classified by an official of a U.S. embassy overseas which was still utilizing the old classification markings and procedures specified in Executive Order 10501.[210] Presumably, other departments and agencies have encountered the same confusion due to the parallel functioning of two vitally different security classification systems caused by the lag in issuance and dissemination of the new regulations.

While a legal question might be raised as to the status of documents that were classified—properly or improperly—under either the old or new Executive order, any effort to deal with the unique nature of such a situation would not be appropriate here. The administrative confusion that is latent in the questionable classification status of perhaps hundreds of thousands of documents during this 64-day hiatus may take months or years to untangle.

Are Domestic Activities Related to Security Classification System?

As has been noted earlier in this report (pages 61–66), one of the most controversial questions raised during the hearings was the reason for the change in the language of section 1 of Executive Order 11652 involving "national defense and foreign relations of the United States (hereinafter collectively termed 'national security')." [211] The matter was further pursued with Mr. Buzhardt of the Defense Department in relation to the exemption language of the Freedom of Information Act (sec. 552(b)(1)) dealing with matters exempt by the act "in the interest of the national defense or foreign policy:" [212]

Mr. MOORHEAD. * * * I would like to get back to this matter of the new Executive order purporting to change the law. The new Executive order reads "by virtue of the authority vested in me, the President, by the Constitution and the statutes of the United States," and the only statute it refers to is 5 U.S.C. 552—the Freedom of Information Act.

[210] These classified documents are contained in a locked security cabinet in the subcommittee office.
[211] Ibid., pp. 2852–2853.
[212] Ibid., pp. 2473–2474.

That act said all documents shall be available to the public with certain exceptions—(b)(1) through (9). And the statutory language of exemption (b)(1) is "national defense and foreign policy."

If the change to the words "national security and foreign relations" is to have any effect, it is an attempt by Executive order to change a statute of the United States.

Where does the Constitution of the United States give the President the authority to change statutes enacted by the Congress and signed into law by the President of the United States?

Mr. BUZHARDT. I do not believe there was any intent or effort in the Executive order to change a statute of the United States.

Mr. MOORHEAD. Then the law of the land remains that all Government documents in this area are available to the public with the nine exemptions, one of which says "national defense and foreign policy." Is that correct?

Mr. BUZHARDT. That remains the applicable law.

Mr. MOORHEAD. Then if that remains the applicable law, why was the language changed in the Executive order?

Mr. BUZHARDT. Mr. Chairman, the language was changed in order to be more precise. Now, let's go back to 10501.

We have seen, and I don't know what the attitude or intent was when 10501 was issued, but it seems quite apparent that many people found things that affected the security of the Nation, or thought they did within the term national defense that made that phrase, if you will, expandable by construction.

National defense as we would think of it in a lay term certainly would not include either foreign policy or foreign relations, but they were protected under that order. So by construction, national defense, the definition in 10501, was interpreted sufficiently broad both in practice and by the courts, in many cases, to include both foreign relations and foreign policy.

Now, once you get people into the habit of construing a term more broadly than you could give it a lay definition, you are almost inviting them to use an unbridled judgment, and I am afraid that has happened under 10501, that it was expanded by construction to the point where it had no definite boundaries. * * *

Mr. MOORHEAD. * * * I seem to be unable to get across to an able lawyer—you keep going back to 10501. A statute signed by the President can affect an Executive order but an Executive order can't repeal or amend a statute and——

Mr. BUZHARDT. I quite agree.

Mr. MOORHEAD. And the Freedom of Information Act was enacted after—signed by the President—some 13 years after 10501 was issued. And this was the action of the Congress and the President, which makes it the highest law of the land, having much more standing than any Executive

order or any resolution just adopted by the House and the Senate and not signed by the President. Yet the Executive order either through inadvertence, and it has no effect, or intentionally, and it still has no effect, uses different language than the statutory language.

Mr. BUZHARDT. It uses different language, Mr. Chairman. That does not mean that it is necessarily in conflict with the language used in the Freedom of Information Act.

Mr. MOORHEAD. If it means the same thing as the words in the Freedom of Information Act, then my suggestion would be we should use that language. If you don't like the language in the Freedom of Information Act, then suggest the changes to us and then we can clear up the law in this matter. That is one of the purposes of these hearings, to see if there are needed amendments to the act. I don't think you can amend any act by an Executive order. So I would say that the courts would have to construe this as meaning exactly the same as the Freedom of Information Act.

Additional efforts were made during the hearings with executive branch witnesses to find the rationale for the substitution of the phrase "national security" in section 1 of Executive Order 11652. In this connection, the question as to whether or not the security classification system could be applied to domestic activities was discussed with witnesses from the Defense and Justice Departments with mixed results: [213]

Mr. MOORHEAD. I will tell you, Mr. Buzhardt, one of the concerns I have is this—does the term "national security" when used in the Executive order, authorize the classification of information dealing with domestic intelligence activities of the military services? I am thinking of the recent Army surveillance of civil rights activities, campus leaders, and even Members of Congress.

Mr. BUZHARDT. No; it does not. It is not intended to expand to the domestic scene and treat that as a security matter, because it would be hard to know how these things could jeopardize really the national security, the things you are talking about.

Now, as you know, we do not reveal or disclose investigative files, but, for an entirely different reason, they are not classified. It is primarily a matter of protecting the individual because in an investigative file you get unevaluated raw information, rumor, many things creep in, and it would be unfair to disseminate this out. We went through this in the 1950's.

Mr. MOORHEAD. That was under a different exemption of the——

Mr. BUZHARDT. It is not classification, nor is there any intent to expand the classification subject matter to those areas, none whatsoever. Specifically not.

Mr. MOORHEAD. I am glad to have that emphatically stated on the record.

[213] Ibid., pp. 2492-2493.

Later in the hearings, then Assistant Attorney General Erickson was also queried on this same matter: [214]

> Mr. MOORHEAD. Mr. Erickson, I think I would like to get the record clear on this point:
>
> Can information concerning domestic intelligence surveillance of, let us say, civil rights leaders, antiwar groups, students, labor leaders, and so forth, be classified under Executive Order 11652?
>
> Mr. ERICKSON. They can be classified if they relate to matters that may properly be characterized as national defense or foreign relations. If their activities are strictly domestic in character and have no aspect which would advocate the overthrow of the Government or otherwise interfere with the existence of our Government as we know it they would not be classified.
>
> Mr. MOORHEAD. So that what we normally think of as the activities of various civil rights leaders, student groups, antiwar groups, would not be subject to classification either under the old Executive order or the new one; is that correct?
>
> Mr. ERICKSON. That is correct; so long as they are strictly domestic in character and have no purpose of overthrowing the Government.

Thus, the clear implication of Mr. Erickson's response indicates that matters affecting domestic activities falling into the broad categories of "national defense and foreign relations," lumped as "national security" in the new Executive order may indeed be subject to classification under the terms of the new order.

Since section 7(c) of Executive Order 11652 imposes upon the Justice Department the responsibility "to render an interpretation of this order with respect to any question arising in the course of its administration," [215] the opinion expressed on this subject by Mr. Erickson, then Deputy Attorney General and the Department's representative on the ICRC, would therefore seem to be the viewpoint that would prevail.

Mr. Buzhardt's statement, seeming to limit the classification application in such domestic situations, is not borne out, however, in the DOD directive implementing Executive Order 11652. Section 159.103 (a)(1)—"Classification-Basic Policy"—reads as follows: [216]

[214] Ibid., p. 2693.
[215] Ibid., pp. 2878-2879.
[216] 37 F.R. 15658.

> (1) Consistent with the foregoing, the use and application of security classification shall be limited to only that information which is truly essential to national security because it provides the United States with (i) A military or defense advantage over any foreign nation or group of nations, or (ii) a favorable foreign relations posture, or (iii) *a defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert;* which could be damaged, minimized, or lost by the unauthorized disclosure or use of the information. (Italic supplied.)

While there are certainly areas in which certain domestic activities of our Government in the intelligence and counterintelligence would require classification under Executive Order 11652, the committee intends to closely monitor through its oversight authority the possible areas of abuse of the order in classifying strictly domestic intelligence collection or surveillance of individuals that are unrelated to "national security" considerations.

VII. THE CLASSIFICATION SYSTEM—HISTORICAL RESEARCH PROBLEMS

The unique problems of scholars and historians seeking access to classified Government documents and records of events are a highly specialized part of the total security classification dilemma. Over the years the subcommittee has received many complaints of governmental abuses and many requests for assistance from researchers who are endeavoring to cope with the vast and complex maze of security restrictions in order to obtain access to various departmental or Archives records for scholarly purposes.

Few would argue with the general premise concerning the overall need of Government to avoid carrying out its certain sensitive operations in a "goldfish bowl," particularly in these days of international tension. Certainly, there can be overwhelming public support for the following broad policy statement contained in the preamble to Executive Order 11652: [217]

> Within the Federal Government there is some official information and material which, because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be subject to some constraints for the security of our Nation and the safety of our people and our allies. To protect against actions hostile to the United States, of both overt and covert nature, it is essential that such official information and material be given only limited dissemination.

Such a statement is even more readily acceptable when it is placed within the context of the first paragraph of Executive Order 11652:

> The interests of the United States and its citizens are best served by making information regarding the affairs of Government readily available to the public. This concept of an informed citizenry is reflected in the Freedom of Information Act and in the current public information policies of the executive branch.

Noted historian Arthur Schlesinger, Jr., pointed out in a recent article that "the functioning of democracy requires some rough but rational balance between secrecy and disclosure, between official control of information and public need for it." [218]

During the past several years, the secrecy policies of Government have become more and more a matter of public attention and concern. Historians, political scientists, journalists, and others have become more interested in the study and analysis of contemporary foreign policy and recent diplomatic history and have protested governmental restrictions on study and research of official records. A report on

[217] Ibid., p. 2312.
[218] Hearings, pt. 7, p. 2297.

scholar's access to Government documents, prepared by the 20th Century Fund earlier this year, describes the broad scope of the problem:[219]

> In essence, the security classification system and other restrictions on access to records permit government officials to control the flow of information to the public. The executive departments, particularly the presidency, can dominate the headlines with official pronouncements, news releases, press conferences, and publication of documents. An administration can even "blow the lid" on its own secrecy, as shown by President Nixon's recent disclosure of the secret negotiations with the North Vietnamese. Off-the-record briefings and leaks to the press permit officials to discuss policy and events—often without taking responsibility for what they reveal. Former officials publish memoirs of their years in office; government departments issue their own histories of significant events; favored scholars and journalists are sometimes given access to official records that remain off limits to others.
>
> In each case, officials or former officials exercise discretion in choosing what to reveal and what to conceal. As a consequence, the public must rely on sources that have some vested interest in the information that is given out.
>
> What the public has not received—or has waited decades for—are accounts of government operations based on first-hand records and commentaries by detached observers. The State Department, which has maintained a thirty-year limit on classification of its files, did not make the official record of American diplomacy in World War II available to the general public until January 1972. The documents on most of our Cold-War diplomacy remain in closed files. The Joint Chiefs of Staff have only recently opened segments of their World War II records, and their postwar files are unavailable for any nonofficial purpose. Few Army records from the post-1945 period are available to unofficial researchers even on a restricted basis. Researchers at the Truman Library in Independence, Missouri, still cannot use some of the secret documents on which Mr. Truman based his memoirs, published in 1958.

The importance of scholarly research access to historical documents in our free society cannot be overemphasized. As one witness, Lloyd C. Gardner, chairman of the history department at Rutgers University, pointed out:[220]

> Historians and other scholars concerned with the reconstruction of the past perform, or should perform, an important service in a democratic society.
>
> Traditionally, historians provide a nation with its memory, but in an open representative society, they are also obligated to sustain a dialog with the government and its policymakers. It is not too much to say that this second aspect of the citizen-scholar's responsibility is an essential part of the definition of an open society.

[219] Carol M. Barker and Matthew H. Fox, "Classified Files: The Yellowing Pages." A report on scholars' access to Government documents. New York: The Twentieth Century Fund: 1972. pp. 4-5.
[220] Hearings, pt. 7, p. 2643.

> Without access to Government documents, however, he cannot function effectively in either capacity. In 1959, as a graduate student researching a book on New Deal diplomacy, I was able, with much difficulty, to see certain files for the years 1940–41. Thirteen years later the latest date open to scholars is only 1945, with certain classified documents still exempted. In those 13 years, scholars have thus lost eight or nine in terms of access.

Mr. Paul L. Ward, executive secretary of the American Historical Association, said:[221]

> Historians and their fellow scholars who have dealt with official documents are fully aware, at the same time, of the human and practical realities surrounding the generation and preservation of records, both official and personal. We recognize the importance for rational decisionmaking and for responsible administration of both putting on paper communications and proposals and of keeping these pieces of paper as records for consultation when related problems thereafter arise. We recognize the threat to these necessary practices when confidentiality for an appropriate time cannot be assured. We would argue, indeed, that the confidence of working administrators in this necessary confidentiality, a confidence so shaken in recent months by a whole series of leaks to the press, cannot be reestablished without a better structure of classification and declassification of documents, a structure that both protects confidentiality while needed and also assures public scrutiny in time enough so that government mistakes do not snowball into self-perpetuating burdens upon our country's minds and energies.

Dr. James B. Rhoads, Archivist of the United States, described the dimensions of the problem that the 38-year-old National Archives faces in this regard in the following terms:[222]

> In the last generation we have grown a great deal. We have become the National Archives and Records Service. We conduct an on-going records management program working with agency officials and their files. We operate 15 Federal Records Centers and six Presidential libraries, in addition to the National Archives itself. We have in our custody approximately 30 billion pages of Federal records, something more than 40 percent of the total volume of the Government's records. But while both our activities and our holdings have expanded, our goals remain the same: to serve the rest of the Government by caring for its non-current records and to serve the public in general by making available the documents of enduring value.
>
> Because of our double mission—serving both the rest of Government and the public—we are particularly sensitive to the problem of restrictions on access to records and other historical materials. We are well aware of the conviction within Government that a degree of confidentiality is essential for the national security and for the proper operation of

[221] Ibid., pp. 2636–2637.
[222] Ibid., pp. 2604–2605.

Government. We are also aware of the equally widespread insistence on the part of historians and other researchers that they receive access to records, for we are most often the first to receive their requests and their complaints.

As we have grown in recent years and as agencies have retired their more recent, 20th century, records, we have increasingly had to face the problem of handling classified documents. This is a difficult problem. Indeed, it is one of the most difficult problems that we in the National Archives and Records Service face.

Dr. Rhoads went on to describe the relationship between researchers, the National Archives, and the handling of classified documents:[223]

* * * There are now six Presidential libraries. All are open for research, and all but one, the Herbert Hoover Library, contain significant quantities of classified material originated by the White House. In the absence of any explicit means in the earlier Executive order for declassification of this material, this has created a very serious and obvious problem. Section 11 of the new Executive order provides an explicit means for the declassification of such documents, most of which have come to rest—and hopefully, will continue to come to rest—in one of our Presidential libraries. This section provides that we can now declassify Presidential and White House classified documents. In doing so, we must observe the guidelines provided by the new Executive order itself in section 5, consult with departments having primary subject matter interest before making a final decision, and observe the terms of the donor's deed of gift. Section 11, contrary to certain comments, does not add new or extra restrictions. In fact, it liberalizes access by providing an explicit, and we believe, effective means of declassifying the all important Presidential and White House documents which hitherto have existed in a kind of classification limbo.

He cited a provision of the new Executive order that he felt would greatly expedite the declassification process by the Archives:[224]

I am aware, Mr. Chairman, that the new Executive order has been described by some as not going far enough. However, there are a number of new elements in the order which would materially hasten the process of declassification.

Section 3(E) of the new order provides that:

> Classified information or material transferred to the General Services Administration for accession into the Archives of the United States shall be downgraded and declassified by the Archivist of the United States in accordance with this order, directives of the President issued through the National Security Council and pertinent regulations of the departments.

[223] Ibid., p. 2607.
[224] Ibid., p. 2606.

> This is new. For the first time the staff of the National Archives and Records Service will have the authority to declassify classified documents. In the past, much time and much paper has been expended in our obtaining authorization from individual agencies to declassify particular records of those agencies. Now, equipped with nothing more than the guidelines that will be provided to us by the agencies and the National Security Council, along with those already spelled out in the new Executive order itself, we can take the action of declassification on our own. This will eliminate the time-consuming delays which so annoy researchers and the paper-producing memos which annoy both those who must write them and those who receive them. * * *

Foreign Relations Series

For many years, the major official documentary series, Foreign Relations of the United States, published by the State Department, has been an indispensable research tool for researchers, historians, and other students of international affairs. There is presently a time lag of some 26 years in the publication of this important series of documents, papers, communiques, and other diplomatic records. Materials now being published related to events taking place through 1947.

On the same day that he issued Executive Order 11652, President Nixon also directed a March 8, 1972, memorandum to the Secretary of Defense, the Director of Central Intelligence, and the Assistant to the President for National Security Affairs calling for an acceleration of the publication of the "Foreign Affairs" series to reduce the time lag to 20 years by 1975, and thereafter to maintain this 20-year publication period.[225] The State Department had initially requested funds for three additional historians and received an additional $112,200 in program funds for fiscal year 1973 for editing, indexing, printing, and other related functions to carry out the President's instructions.[226] Such actions have the support of the leading academic groups involved in the field.

In addition, the Advisory Committee on Foreign Relations of the United States—made up of scholars representing the American Political Science Association, the American Society of International Law, and the American Historical Association—recommended at its November 5, 1971, meeting that the State Department publish collections of documents relating to the major international crises since 1946 substantially before those events would be covered in the regular chronological "Foreign Relations" series.[227]

[225] See ibid., pp. 2650–2651 for text of President Nixon's memorandum.
[226] Ibid., p. 2651; the outlines of the Foreign Relations series publications for 1947–1950 and a status report on their progress is also provided here.
[227] Ibid., pp. 2647–2649 for text of Advisory Committee report.

The Committee feels that such a recommendation would be consistent with the overall objectives of accelerating the public's access to foreign relations information and would also serve the Nation by providing more current insights into our foreign policy decisions in recent history that would be valuable to current foreign policy judgments of responsible executive branch officials as well as to Congress and scholars and the public as a whole.

This view was well summarized by comments by Mr. Gardner: [228]

> Nations, like individuals, depend in part upon memory in order to be able to function rationally in the present. Historians are to a degree responsible for what stands out in a nation's memory; they supply experience longer than one generation's lifespan, and broader than that of any group of individuals.
>
> As one approaches the present, the historian's most valuable asset, perspective, is diminished chronologically, and in a secrecy-conscious nation, by the lack of available evidence as well.
>
> The Nation's memory is thus weakest for the years of the recent past, a serious defect, unless one is prepared to concede that the public should reach its conclusions on the basis of little or no information, or that the policymaker is the only one who needs the memory.

[228] Ibid., p. 2657.

VIII. SECURITY CLASSIFICATION SYSTEM—EXECUTIVE ORDER VERSUS STATUTE

One of the major areas of study during the hearings on the operation of the security classification system and its relationship to the people's "right to know"—as exemplified in the Freedom of Information Act—was whether the system can effectively operate under any Executive order arrangement or whether Congress should, in the exercise of its constitutional authority, enact a statutory system to govern all security classification functions.

A great many viewpoints on this question were expressed by the expert witnesses who testified:

Former Ambassador and Supreme Court Justice Goldberg:

> I think as a general principle, I would say that Congress has the right to prescribe the principles under which material is classified and declassified. * * * Congress could take away from the Executive, which is the author of the document, the right to make the decision about declassification. It could entrust it to a quasi-judicial group or some agency divorced from the group which does the classification itself.[229]

The constitutional prerogative to legislate in the field was also discussed by Congressman Moss and then Assistant Attorney General Rehnquist, now a Supreme Court Justice: [230]

> Mr. Moss. Certainly, if the Congress were to enact a statute which spelled out a system of classification and specified that be the only system of classification, that would dominate, or do away with the classification under Executive Order 10501, wouldn't it?
>
> Mr. REHNQUIST. Yes; I think Congress could supersede Executive Order 10501 so long as it didn't infringe on the constitutional prerogatives of the President.* * *

Retired Air Force security classification expert William G. Florence:

> * * * It is clearly within the responsibility of Congress to correct the abuses of administrative power now being exercised under the existing security classification system in Executive Order 10501, and which can be expected to continue under Executive Order 11652. * * * The most suitable legislative action would be the enactment of a law to accomplish the purpose of Executive Orders 10501 and 11652, and at the same time serve the interests of Congress and the people regarding access to information. Any reasonable legislation that would provide a framework of law instead of

[229] Hearings, pt. 5, p. 1450.
[230] Hearings, pt. 2, p. 381.

an administrative regulation in which to protect such national defense information as can and ought to be protected would be a very worthwhile improvement. * * * [231]

* * * * *

Historian Lloyd C. Gardner:

As an alternative to the Executive order system, I would suggest a law providing for automatic declassification of documents after 15 years. The real key to attacking this problem by legislation is, however, to change the present categories to spell out what may or may not be classified militarily and politically.

Thus, "top secret" presently covers military secrets such as weapons systems and strategic battle plans, as well as political decisions. These are very different problems and must be handled differently.

But a 30-year rule is plainly incompatible with any serious definition of responsible citizenry in a democracy. The historian will always write, make judgments, and draw conclusions. But these will be less useful to the country until he has access to Government files.

One can argue, and historians differ, about what rule should prevail—an 8-year, 10-year, 15-year, or 20-year, automatic declassification procedure.

An Executive order, no matter how seriously intended, cannot substitute for congressional legislation. Even with such legislation, moreover, Congress will have to insure that something is done to carry out its will, probably through the creation of a committee or commission composed of representatives of the executive and legislative branches, and including private citizens.

A legislative solution is the only long-range alternative in keeping with a representative form of government. * * * [232]

Dr. Paul Ward, executive secretary of the American Historical Association, also stated that "our association position would heartily support" constructive and workable security classification legislation in the Congress.[233]

Several Members of Congress who testified also supported the concept of a statutory security classification system:

Congressman Sam Gibbons:

Congress should enact legislation providing a clear definition of national security matters which can be classified and the circumstances under which such classification should be imposed.[234]

In response to a question by Congressman Moss as to who should impose the guidelines for classifying, the Executive or the Congress, Congressman Bob Eckhardt responded: [235]

[231] Hearings, pt. 7, pp. 2538–2539; for details of criteria or statute recommended by Mr. Florence, see pp. 2539–2540.
[232] Ibid., p. 2657.
[233] Ibid., p. 2640.
[234] Hearings, pt. 1, p. 203.
[235] Ibid., p. 221.

> Mr. ECKHARDT. Well, of course, Congress always has the right to do it. But let me say this: I think classification should be for the purposes of determining whether an executive officer should respect a confidence and I think in that respect there is nothing wrong with Congress setting out guidelines and directing the executive department to follow them. * * *

Senator Mike Gravel:

> One of Congress' most urgent tasks is to replace Executive Order 11652 with legislation regulating the classification process. At a minimum, specific language is required to insure that the classification system is applied only to information that, if disclosed, would definitely endanger our national defense posture. * * * [236]

It is reasonable to expect differences of opinion, even among those who support the concept of a statutory security classification system, as to the precise scope and detail of such legislation.

The Atomic Energy Commission's Statutory Classification System

Only one Federal agency, the Atomic Energy Commission (AEC), operates under a separate statutory security classification system. In an endeavor to determine just how well AEC's system has functioned, the subcommittee called for testimony from the AEC Director of Classification, Mr. Charles Marshall.[237]

Section 142 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2162), provides for a system that is unique in the executive branch—a statutory basis for the classification and declassification of AEC information known as "restricted data." This statutory system operates within the framework of the old Executive Order 10501 and the present Order 11652 and classification categories of the Executive order are also applicable to AEC.

Mr. Marshall outlined the broad way in which the Atomic Energy Act deals with problems involving security classification: [238]

> The Atomic Energy Act also includes a mandate on how to deal with the basic problem we are discussing today; namely, the problem of assuring that information important to the national security is adequately protected while all other information is fully and freely disseminated. It stipulates that (1) the Commission is to safeguard restricted data in such a manner as to assure the common defense and security; and (2) the Commission is to declassify as much of this information as national security permits so as to facilitate the free interchange of ideas and criticism which is essential to scientific and industrial progress and to public understanding.

He went on to point out:

> The Atomic Energy Commission was established by the Atomic Energy Act of 1946 and has functioned since then to

[236] Hearings, pt. 7, p. 2561.
[237] Mr. Marshall's testimony begins on page 2574 of pt. 7 of the hearings.
[238] Ibid., pp. 2574-2575.

carry out its mandates. The act, which underwent a significant revision in 1954, prescribes specific requirements for the handling of atomic energy information. Subsection 11.y. defines restricted data as:

> All data concerning (1) design, manufacture or utilization of atomic weapons; (2) the production of nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the restricted data category pursuant to section 142.

In effect, this definition classifies atomic energy information from its inception and it affects not only Government-generated information but information generated by all citizens of the United States. This represents a basic difference between the Atomic Energy Act and the Executive order which applies only to Government operations. Both, however, are seriously concerned with accomplishing declassification of information as soon as national security permits. Section 142 of our act in its turn prescribes the means for removing information from the restricted data category either by declassification or other means.

Classification Director Marshall explained that AEC's classification and declassification program, based primarily on the Atomic Energy Act provisions, utilizes "detailed classification guides which define that information which warrants classification and that information which does not and is therefore unclassified." "These guides are continuously reviewed and revised as necessary," he stated, "to insure that they are consistent with current circumstances."[239] He also added:

> In classifying information there are really two decisions that need to be made, the first, whether or not the information should be classified; that is, whether or not it warrants some protection; the second decision is what level of classification shall be applied; that is, what level of protection the information requires. In the case of restricted data and formerly restricted data, the Atomic Energy Act makes that first decision. The second one, including the declassification, is made by the AEC.

Mr. Marshall stated that "to carry out its classification and declassification program, the AEC keeps abreast of the technical developments thoughout the world in all of the areas of information in which the AEC has an interest." AEC's Division of Classification has as its mission "to insure that only that information which warrants protection from the point of view of the national defense and security will continue to be classified and that all other information will be declassified and made available for general use."[240]

He continued:

> As a result of AEC declassification actions only a very few programs are now classified in any significant way. These include the weapons program and the program for the separation of fissionable isotopes. Most other programs are either

[239] Ibid., p. 2575.
[240] Ibid., p. 2576.

completely unclassified or nearly so. For example, information concerning production reactors, space propulsion, space power and controlled thermonuclear reactors is almost completely unclassified. Programs for basic scientific research, medical, biological, and agricultural applications, civilian power reactors and civilian research reactors are all completely unclassified.

Great emphasis is placed on the declassification of documents, carried out by "designated responsible reviewers," who are scientists in various technical fields. They systematically review classified material to determine, within current classification guides, whether or not particular documents still need to be classified.[241] As a result, Mr. Marshall stated, more than 650,000 documents have been declassified under a "special review program" begun in July 1971.

Congressman Chet Holifield, chairman of this committee, a member of the Joint Atomic Energy Committee since its creation in 1946, and several times chairman of the Joint Committee, explained the background of the AEC classification policies during the hearings:[242]

In the early days of the Manhattan project, before and during World War II, up until ending the war in 1946, and going on up to 1954, about the sole really major program of the Atomic Energy Commission was in the field of producing and improving weapons for our national defense. During that period there was pretty tight security because weapon production was the only thing that we were really stressing at the time.

In 1954, when the complete revision of the act occurred a new policy was adopted, at the behest of the committee, because we recognized that this great new source of energy could have blessings for mankind as well as the threat of destruction of mankind. So we at that time began to accelerate the peacetime applications and in so doing we found that it was necessary to declassify a great many of the procedures and a great many of the classified documents because in most instances they also had peacetime applications. Wherever it was possible we declassified these documents which consisted mostly of information of how to use atomic energy, and use it safely, and how to provide it. In some instances where there was double meaning to a piece of information, in other words, it could be used for either peacetime applications or for the weapon program, we had to go rather slowly and declassify bit by bit.

But the policy from 1954 of the Joint Committee was that we wanted to get everything out in the open that we could, because in the first place it had been produced by taxpayers' money and if there was peacetime application we wanted it used to the utmost.

In the second place, we had a tremendous body of scientists working on this project and the scientists inherently

[241] Ibid.
[242] Ibid., p. 2578.

believe in declassification because they believe in the freedom and dissemination of knowledge, particularly scientific new areas of knowledge. So we had no inherent opposition from the scientists and the laboratory directors.

This enabled us to go forward in harmony with the committee's desires and the operation of the different laboratories, and we found that, as Mr. Marshall's statement says here, we could declassify literally thousands and even hundreds of thousands of pages of otherwise classified material. Today I would say that there is a very small, relatively small field of classification.

Subcommittee Chairman Moorhead, in reviewing the AEC's statutory classification system, observed: [213]

> It is important to note that the AEC information program, as well as its security classification procedures, have seemed to work exceptionally well. We are aware of the extremely sensitive types of classified information which fall within the AEC's jurisdictional responsibility. The operational experience gained over many years through the AEC security classification system is of particular interest to this subcommittee since legislation will soon be introduced and considered here that would replace the Executive order approach by a statutory security classification system throughout the executive branch of Government.
>
> We have studied the operation of your system, Mr. Marshall, and have noted its many advantages. * * *

Like other executive agencies the AEC also functions within the Executive order classification system, as well as its own statutory system. The committee notes, however, the sharp contrast between the apparent efficient operation of the AEC classification system and the administrative failures that have marked the operation of the Executive order system during the past 20 years.

It is true that the highly technical type of information that is subject to classification within AEC's own statutory system and its limited scope of applicability makes it more manageable. Moreover, scientific development in the atomic energy field usually provides more precise benchmarks for measuring the necessity to continue classification of AEC information at a particular level than is generally true in the fields of foreign policy or defense information. This means that AEC's system of constant review of its "restricted data" in the light of changing technology and its ongoing emphasis on downgrading and declassification of data when it no longer requires protection makes its statutory system more administratively sound and workable.

The committee intends to make further studies of the AEC statutory classification model in the hope that it will provide additional insights into ways in which a statutory classification system may be developed to apply throughout the executive branch of government.

[213] Ibid., pp. 2573–2574.

IX. CONCLUSIONS

For well over a decade the Government Operations Committee has conducted in-depth studies and investigations and has held months of hearings now covering many thousands of printed pages of testimony. It has issued more than a dozen reports and other publications dealing with many of the complex aspects of the Nation's security classification system as it has operated under various Executive orders during the past five administrations.

Over the years, the committee's findings and conclusions have documented widespread overclassification, abuses in the use of the classification stamps, and other serious defects in the operation of the security classification system. These committee documents have revealed dangerous shortcomings of a system that has been administratively loose and uncoordinated, unenforced and perhaps unenforceable. It has functioned in a way to deny public access to essential information. It has spawned a strangling mass of classified documents that finally weakened and threatened a breakdown of the entire system.

These same committee reports have repeatedly made constructive recommendations to executive agencies to help correct the administrative and judgmental deficiencies of the security classification system. Unfortunately for the integrity of the system and for the taxpayers who must pay millions of dollars annually to keep the classification machine running, many of these recommendations have gone unheeded.

The committee believes that there is an unquestioned need for Federal agencies to avoid the release or dissemination to the public of certain sensitive types of information, the safeguarding of which is truly vital to protecting the national defense and to maintain necessary confidentiality of dealings between our country and foreign nations.

The committee also believes, however, that the Nation is strengthened when the American public is informed on matters involving our international commitments and defense posture to the maximum extent possible, consistent with our overriding security requirements. Our fundamental liberties are endangered whenever abuses in the security system occur. Within these constraints, when information that should be made available to the people is unnecessarily withheld by government—for whatever the reason—our representative system is undermined and our people become less able to judge for themselves the stewardship of government officials. Information is essential to knowledge—and knowledge is the basis for political power. Under our governmental system, maximum access to information must, therefore, always reside firmly in the hands of the American people.

The efficiency and integrity of a security classification system, whether established by Executive order or statute, ultimately rests in large part on proper use of clearly defined gradations of secrecy. Unnecessary classification of marginal information and overclassification must be strictly avoided. When the mass of currently used

classified information aggregates many millions of pages—much of which is overclassified—there no longer can be the degree of respect or selectivity upon which classification markings depend for their integrity. To the extent that any classification system does not punish those of its participating officials who abuse the system, who classify unnecessarily, or who "play it safe" by overclassifying, it adds immeasurably to the proliferation of classified documents, gradually weakening and eventually destroying the integrity and effectiveness of the entire system. Such abuses undermine the ultimate ability of the system to adequately safeguard those highly sensitive and vital secrets upon which the security of our Nation and its people may well depend.

Among the essential elements for the efficient operation of any security classification system are the procedures established for the systematic downgrading and rapid declassification of all classified information when the need for its protection has ceased to exist. Such circumstances are not so much measurable in time periods as they are geared to the rapidly moving sequence of events involving scientific development, defense technology, changing diplomatic situations, and the like.

Any security classification system should provide precise definitions of truly vital categories of information subject to classification and also have an effective mechanism for strictly limiting classification authority among Federal departments and agencies involved in national defense and foreign policy matters, and among the key policymaking officials. These officials should be identified on documents they classify; they should be held *strictly* accountable for their classification judgments; and they should be disciplined for abuse of their authority. Otherwise, the system will be compromised and the volume of unnecessarily classified and overclassified information will overwhelm those who stamp it.

Finally, an effective security classification system should certainly have a vigorously enforced mechanism for reviewing and policing its own operations to assure that the system does not compromise vital defense or foreign policy secrets, does not abuse the public's right to know, nor founder in its own bureaucratic excesses. Another safeguard should be full judicial review of classification decisions. The system should therefore include a requirement for in camera examination of classified information by the Federal courts in cases involving disputes over classification markings so as to legally determine whether or not such information is properly classified.

In the past administration of security classification systems established by Executive orders, these and other basic criteria for the ultimate success of the system have been notably absent, or have not been properly implemented or enforced.

The committee also notes that while an updating of the *Foreign Relations* series—ordered by President Nixon in March 1972—is a forward step, such action should be further accelerated and additional resources earmarked for this purpose. Serious consideration should be given to the proposal of the leading academic groups calling for the State Department to publish in advance of the *Foreign Relations* series collections of documents relating to the major international crises since 1947.

Executive Order 11652, issued on March 8, 1972, has been labeled the "first major overhaul of our classification system since 1953." The result of some 14 months of executive consideration by an interagency committee headed by former Assistant Attorney General William H. Rehnquist, the new order attempts to deal with some of the serious defects in the security classification system that became so obvious in the operation of Executive Order 10501.

For example, there has been an announced reduction of some 31,000 persons in executive departments and agencies authorized to classify documents as "Top Secret", "Secret", or "Confidential" under the new Executive order—a drop of 63 percent. However, the committee has yet been unable to verify this claim. The number of executive departments and agencies authorized to classify has been reduced from 37 to 25, exclusive of the Executive Office of the President. An Interagency Classification Review Committee, headed by Ambassador John Eisenhower, has been created to monitor the administration of the new order. The order makes an effort to tighten up the security classification categories, endeavors to promote the speedier downgrading and declassification of information, and makes a slight reduction—from 12 to 10 years—in length of the normal declassification schedule from the "Top Secret" level.

However, as has been pointed out previously in this report at pages 58–87, serious shortcomings in the new order have already surfaced—some inherent in the language of its provisions and some in the procedural aspects involving its design, promulgation, and in the issuance of implementing regulations. They may be summarized briefly as follows:

1. Among the major defects inherent in the language of the new order are the following provisions, which were discussed previously on pages 61–80 of this report and include:

(*a*) the change of basic terminology of the order's application—from "national defense or foreign policy" to "national defense or foreign *relations*", referred to in the new order as "national security";

(*b*) the lack of sufficiently strong penalties for overclassification;

(*c*) the lack of assurance to guarantee Congress the full authority to properly exercise its oversight and investigative responsibilities regarding the operation of the new Executive order;

(*d*) the legitimization of dozens of access or control markings that apply to classified or unclassified data; and

(*e*) loopholes in the mandatory review provisions affecting the declassification of exempt classified information.

2. The appropriate committees of the Congress having extensive experience and expertise in the oversight of the security classification system were not given the opportunity by the executive branch to comment on the design of the new Executive order. The Foreign Operations and Government Information Subcommittee of this committee, with more than 17 years of vigorous oversight and constructive criticism of the present system, was refused the opportunity to informally study and comment upon the draft Executive order.

3. There was an administrative lag between the effective date of the new order and its implementation by affected executive departments and agencies. Only six of them had issued regulations some 64

days after the effective date of the new order. Another three affected agencies published such regulations in October 1972, while an additional four came out in November, eight more in December, and the final four agencies finally published their implementing regulations in January 1973. This was despite clear warnings by the subcommittee during the hearings that, since the order was issued prematurely, there should be a postponement of the effective date to provide for the orderly transition from the old system to the new.

The new order omitted a "savings clause" that would have protected against legal questions being raised concerning the status of information classified after the effective date of the new order, but *before* agency regulations could be written, promulgated, and implemented.

4. Conflicting interpretations were given by executive branch witnesses over the extent to which "domestic surveillance" activities by Federal agencies involving American citizens are subject to classification under the new Executive order.

5. Provisions of the new order affecting the access of historians, researchers, and scholars to classified data of the post-World War II period fall far short of the policies necessary to permit the Congress or the public to benefit from historical insights into defense and foreign policy decisions of this crucial period of U.S. involvement in global crises.

Finally, the committee concludes that the statutory security classification system, as operated by the Atomic Energy Commission, with its clear classification guides, its emphasis on continuing review of classified information, and its resulting capability to declassify and make public large amounts of previously classified material each year contains most of the positive elements of a model security classification system. It should receive further study when additional consideration is given to the establishment of a statutory classification system.

A statutory system should be established, perhaps as an amendment to the Freedom of Information Act, to make it clear that Congress intends a proper balancing between the safeguarding of information classified under strict guidelines to protect vital defense and foreign policy secrets and the right of the American public to know how the affairs of their government are being conducted. Congress should also take this necessary action to assure maximum credibility of all citizens in our governmental institutions and in our elected and appointed officials.

X. RECOMMENDATION

The committee therefore strongly recommends that legislation providing for a statutory security classification system should be considered and enacted by the Congress. It should apply to all executive departments and agencies responsible for the classification, protection, and ultimate declassification of sensitive information vital to our Nation's defense and foreign policy interests. Such a law should clearly reaffirm the right of committees of Congress to obtain all classified information held by the executive branch when, in the judgment of the committee, such information is relevant to its legislative or investigative jurisdiction. The law should also make certain that committees of Congress will not be impeded in the full exercise of their oversight responsibilities over the administration and operation of the classification system.

APPENDIX

EXECUTIVE ORDERS NOS. 11652 AND 11714

THE WHITE HOUSE

March 8, 1972.

EXECUTIVE ORDER NO. 11652

CLASSIFICATION AND DECLASSIFICATION OF NATIONAL SECURITY INFORMATION AND MATERIAL

The interests of the United States and its citizens are best served by making information regarding the affairs of Government readily available to the public. This concept of an informed citizenry is reflected in the Freedom of Information Act and in the current public information policies of the executive branch.

Within the Federal Government there is some official information and material which, because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be subject to some constraints for the security of our Nation and the safety of our people and our allies. To protect against actions hostile to the United States, of both an overt and covert nature, it is essential that such official information and material be given only limited dissemination.

This official information or material, referred to as classified information or material in this order, is expressly exempted from public disclosure by section 552(b)(1) of title 5, United States Code. Wrongful disclosure of such information or material is recognized in the Federal Criminal Code as providing a basis for prosecution.

To insure that such information and material is protected, but only to the extent and for such period as is necessary, this order identifies the information to be protected, prescribes classification, downgrading, declassification, and safeguarding procedures to be followed, and establishes a monitoring system to insure its effectiveness.

Now, therefore, by virtue of the authority vested in me by the Constitution and statutes of the United States, it is hereby ordered:

SECTION 1. SECURITY CLASSIFICATION CATEGORIES

Official information or material which requires protection against unauthorized disclosure in the interest of the national defense or foreign relations of the United States (hereinafter collectively termed "national security") shall be classified in one of three categories, namely, "Top Secret," "Secret," or "Confidential," depending upon the degree of its significance to national security. No other categories shall be used to identify official information or material as requiring protection in the interest of national security, except as otherwise expressly provided by statute. These classification categories are defined as follows:

(A) *"Top Secret."*—"Top Secret" refers to that national security information or material which requires the highest degree of protection. The test for assigning "Top Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Examples of "exceptionally grave damage" include armed hostilities against the United States or its allies; disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans or complex cryptologic and communications intelligence systems; the revelation of sensitive intelligence operations; and the disclosure of scientific or technological developments vital to national security. This classification shall be used with the utmost restraint.

(B) *"Secret."*—"Secret" refers to that national security information or material which requires a substantial degree of protection. The test for assigning "Secret" classification shall be whether its unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Examples of "serious damage" include disruption of foreign relations significantly affecting the national security; significant impairment of a program or poliyc directly related to the national security; revelation of significant military plans of intelligence operations; and compromise of significant scientific or technological developments relating to national security. The classification "Secret" shall be sparingly used.

(C) *"Confidential."*—"Confidential" refers to the national security information or material which requires protection. The test for assigning "Confidential" classification shall be whether its unauthorized disclosure could reasonably be expected to cause damage to the national security.

SECTION 2. AUTHORITY TO CLASSIFY

The authority to originally classify information or material under this order shall be restricted solely to those offices within the executive branch which are concerned with matters of national security, and shall be limited to the minimum number absolutely required for efficient administration. Except as the context may otherwise indicate the term "Department" as used in this order shall include agency or other governmental unit.

(A) The authority to originally classify information or material under this order as "Top Secret" shall be exercised only by such officials as the President may designate in writing and by:

(1) The heads of the Departments listed below;

(2) Such of their senior principal deputies and assistants as the heads of such Departments may designate in writing; and

(3) Such heads and senior principal deputies and assistants of major elements of such Departments, as the heads of such Departments may designate in writing.

Such offices in the Executive Office of the President as the President may designate in writing.

Central Intelligence Agency.
Atomic Energy Commission.
Department of State.
Department of the Treasury.
Department of Defense.
Department of the Army.
Department of the Navy.
Department of the Air Force.
United States Arms Control and Disarmament Agency.
Department of Justice.
National Aeronautics and Space Administration.
Agency for International Development.

(B) The authority to originally classify information or material under this order as "secret" shall be exercised only by:

(1) Officials who have "top secret" classification authority;

(2) Such subordinates as officials with "top secret" classification authority under (A)(1) and (2) above may designate in writing; and

(3) The heads of the following named departments and such senior principal deputies or assistants as they may designate in writing.

Department of Transportation.
Federal Communications Commission.
Export-Import Bank of the United States.
Department of Commerce.
U.S. Civil Service Commission.
U.S. Information Agency.
General Services Administration.
Department of Health, Education, and Welfare.
Civil Aeronautics Board.
Federal Maritime Commission.
Federal Power Commission.
National Science Foundation.
Overseas Private Investment Corp.

(C) The authority to originally classify information or material under this order as "confidential" may be exercised by officials who have "top secret" or "secret" classification authority and such officials as they may designate in writing.

(D) Any department not referred to herein and any department or unit established hereafter shall not have authority to originally classify information or material under this order, unless specifically authorized hereafter by an Executive order.

SECTION 3. AUTHORITY TO DOWNGRADE AND DECLASSIFY

The authority to downgrade and declassify national security information or material shall be exercised as follows:

(A) Information or material may be downgraded or declassified by the official authorizing the original classification, by a successor in capacity or by a supervisory official of either.

(B) Downgrading and declassification authority may also be exercised by an official specifically authorized under regulations issued by the head of the Department listed in sections 2(A) or (B) hereof.

(C) In the case of classified information or material officially transferred by or pursuant to statute or Executive order in conjunction with a transfer of function and not merely for storage purposes, the receiving Department shall be deemed to be the originating Department for all purposes under this order including downgrading and declassification.

(D) In the case of classified information or material not officially transferred within (C) above, but originated in a Department which has since ceased to exist, each Department in possession shall be deemed to be the originating Department for all purposes under this order. Such information or material may be downgraded and declassified by the Department in possession after consulting with any other Departments having an interest in the subject matter.

(E) Classified information or material transferred to the General Services Administration for accession into the Archives of the United States shall be downgraded and declassified by the Archivist of the United States in accordance with this order, directives of the President issued through the National Security Council and pertinent regulations of the Departments.

(F) Classified information or material with special markings, as described in section 8, shall be downgraded and declassified as required by law and governing regulations.

SECTION 4. CLASSIFICATION

Each person possessing classifying authority shall be held accountable for the propriety of the classifications attributed to him. Both unnecessary classification and overclassification shall be avoided. Classification shall be solely on the basis of national security considerations. In no case shall information be classified in order to conceal inefficiency or administrative error, to prevent embarrassment to a person or Department, to restrain competition or independent initiative, or to prevent for any other reason the release of information which does not require protection in the interest of national security. The following rules shall apply to classification of information under this order:

(A) *Documents in general.*—Each classified document shall show on its face its classification and whether it is subject to or exempt from the general declassification schedule. It shall also show the office of origin, the date of preparation and classification and, to the extent practicable, be so marked as to indicate which portions are classified, at what level, and which portions are not classified in order to facilitate excerpting and other use. Material containing references to classified materials, which references do not reveal classified information, shall not be classified.

(B) *Identification of classifying authority.*—Unless the Department involved shall have provided some other method of identifying the individual at the highest level that authorized classification in each case, material classified under this order shall indicate on its face the identity of the highest authority authorizing the classification. Where the individual who signs or otherwise authenticates a document or item has also authorized the classification, no further annotation as to his identity is required.

(C) *Information or material furnished by a foreign government or international organization.*—Classified information or material furnished to the United States

by a foreign government or international organization shall either retain its original classification or be assigned a U.S. classification. In either case, the classification shall assure a degree of protection equivalent to that required by the government or international organization which furnished the information or material.

(D) *Classification responsibilities.*—A holder of classified information or material shall observe and respect the classification assigned by the originator. If a holder believes that there is unnecessary classification, that the assigned classification is improper, or that the document is subject to declassification under this order, he shall so inform the originator who shall thereupon reexamine the classification.

SECTION 5. DECLASSIFICATION AND DOWNGRADING

Classified information and material, unless declassified earlier by the original classifying authority, shall be declassified and downgraded in accordance with the following rules:

(A) *General declassification schedule.*

(1) *"Top secret."*—Information or material originally classified "top secret" shall become automatically downgraded to "secret" at the end of the second full calendar year following the year in which it was originated, downgraded to "confidential" at the end of the fourth full calendar year following the year in which it was originated, and declassified at the end of the tenth full calendar year following the year in which it was originated.

(2) *"Secret."*—Information and material originally classified ' secret" shall become automatically downgraded to "confidential" at the end of the second full calendar year following the year in which it was originated, and declassified at the end of the eighth full calendar year following the year in which it was originated.

(3) *"Confidential."*—Information and material originally classified "confidential" shall become automatically declassified at the end of the sixth full calendar year following the year in which it was originated.

(B) *Exemptions from general declassification schedule.*—Certain classified information or material may warrant some degree of protection for a period exceeding that provided in the general declassification schedule. An official authorized to originally classify information or material "top secret" may exempt from the general declassification schedule any level of classified information or material originated by him or under his supervision if it falls within one of the categories described below. In each case such official shall specify in writing on the material the exemption category being claimed and, unless impossible, a date or event for automatic declassification. The use of the exemption authority shall be kept to the absolute minimum consistent with national security requirements and shall be restricted to the following categories:

(1) Classified information or material furnished by foreign governments or international organizations and held by the United States on the understanding that it be kept in confidence.

(2) Classified information or material specifically covered by statute, or pertaining to cryptography, or disclosing intelligence sources or methods.

(3) Classified information or material disclosing a system, plan, installation, project or specific foreign relations matter the continuing protection of which is essential to the national security.

(4) Classified information or material the disclosure of which would place a person in immediate jeopardy.

(C) *Mandatory review of exempted material.*—All classified information and material originated after the effective date of this order which is exempted under (B) above from the general declassification schedule shall be subject to a classification review by the originating department at any time after the expiration of 10 years from the date of origin provided: (1) A department or member of the public requests a review; (2) the request describes the record with sufficient particularity to enable the department to identify it; and (3) the record can be obtained with only a reasonable amount of effort.

Information or material which no longer qualifies for exemption under (B) above shall be declassified. Information or material continuing to qualify under (B) shall be so marked and, unless impossible, a date for automatic declassification shall be set.

(D) *Applicability of the general declassification schedule to previously classified material.*—Information or material classified before the effective date of this

order and which is assigned to group 4 under Executive Order No. 10501, as amended by Executive Order No. 10964, shall be subject to the general declassification schedule. All other information or material classified before the effective date of this order, whether or not assigned to groups 1, 2, or 3 of Executive Order No. 10501, as amended, shall be excluded from the general declassification schedule. However, at any time after the expiration of 10 years from the date of origin it shall be subject to a mandatory classification review and disposition under the same conditions and criteria that apply to classified information and material created after the effective date of this order as set forth in (B) and (C) above.

(E) *Declassification of Classified Information or Material After 30 Years.*—All classified information or material which is 30 years old or more, whether originating before or after the effective date of this order, shall be declassified under the following conditions:

(1) All information and material classified after the effective date of this order shall, whether or not declassification has been requested, become automatically declassified at the end of 30 full calendar years after the date of its original classification except for such specifically identified information or material which the head of the originating department personally determines in writing at that time to require continued protection because such continued protection is essential to the national security or disclosure would place a person in immediate jeopardy. In such case, the head of the department shall also specify the period of continued classification.

(2) All information and material classified before the effective date of this order and more than 30 years old shall be systematically reviewed for declassification by the Archivist of the United States by the end of the 30th full calendar year following the year in which it was originated. In his review, the Archivist will separate and keep protected only such information or material as is specifically identified by the head of the department in accordance with (E)(1) above. In such case, the head of the department shall also specify the period of continued classification.

(F) *Departments Which Do Not Have Authority for Original Classification.*—The provisions of this section relating to the declassification of national security information or material shall apply to departments which, under the terms of this order, do not have current authority to originally classify information or material, but which formerly had such authority under previous Executive orders.

SECTION 6. POLICY DIRECTIVES ON ACCESS, MARKING, SAFEKEEPING, ACCOUNTABILITY, TRANSMISSION, DISPOSITION, AND DESTRUCTION OF CLASSIFIED INFORMATION AND MATERIAL

The President, acting through the National Security Council, shall issue directives which shall be binding on all departments to protect classified information from loss or compromise. Such directives shall conform to the following policies:

(A) No person shall be given access to classified information or material unless such person has been determined to be trustworthy and unless access to such information is necessary for the performance of his duties.

(B) All classified information and material shall be appropriately and conspicuously marked to put all persons on clear notice of its classified contents.

(C) Classified information and material shall be used, possessed, and stored only under conditions which will prevent access by unauthorized persons or dissemination to unauthorized persons.

(D) All classified information and material disseminated outside the executive branch under Executive Order No. 10865 or otherwise shall be properly protected.

(E) Appropriate accountability records for classified information shall be established and maintained and such information and material shall be protected adequately during all transmissions.

(F) Classified information and material no longer needed in current working files or for reference or record purposes shall be destroyed or disposed of in accordance with the records disposal provisions contained in chapter 33 of title 44 of the United States Code and other applicable statutes.

(G) Classified information or material shall be reviewed on a systematic basis for the purpose of accomplishing downgrading, declassification, transfer, retirement, and destruction at the earliest practicable date.

SECTION 7. IMPLEMENTATION AND REVIEW RESPONSIBILITIES

(A) The National Security Council shall monitor the implementation of this order. To assist the National Security Council, an Interagency Classification Review Committee shall be established, composed of representatives of the Departments of State, Defense, and Justice, the Atomic Energy Commission, the Central Intelligence Agency, and the National Security Council staff and a chairman designated by the President. Representatives of other departments in the executive branch may be invited to meet with the committee on matters of particular interest to those departments. This committee shall meet regularly and on a continuing basis shall review and take actions to insure compliance with this order, and in particular:

(1) The committee shall oversee department actions to insure compliance with the provisions of this order and implementing directives issued by the President through the National Security Council.

(2) The committee shall, subject to procedures to be established by it, receive, consider and take action on suggestions and complaints from persons within or without the Government with respect to the administration of this order, and in consultation with the affected department or departments assure that appropriate action is taken on such suggestions and complaints.

(3) Upon request of the committee chairman, any department shall furnish to the committee any particular information or material needed by the committee in carrying out its functions.

(B) To promote the basic purposes of this order, the head of each department originating or handling classified information or material shall:

(1) Prior to the effective date of this order submit to the Interagency Classification Review Committee for approval a copy of the regulations it proposes to adopt pursuant to this order.

(2) Designate a senior member of his staff who shall insure effective compliance with and implementation of this order and shall also chair a departmental committee which shall have authority to act on all suggestions and complaints with respect to the department's administration of this order.

(3) Undertake an initial program to familiarize the employees of his department with the provisions of this order. He shall also establish and maintain active training and orientation programs for employees concerned with classified information or material. Such programs shall include, as a minimum, the briefing of new employees and periodic reorientation during employment to impress upon each individual his responsibility for exercising vigilance and care in complying with the provisions of this order. Additionally, upon termination of employment or contemplated temporary separation for a 60-day period or more, employees shall be debriefed and each reminded of the provisions of the criminal code and other applicable provisions of law relating to penalties for unauthorized disclosure.

(C) The Attorney General, upon request of the head of a department, his duly designated representative, or the chairman of the above described committee, shall personally or through authorized representatives of the Department of Justice render an interpretation of this order with respect to any question arising in the course of its administration.

SECTION 8. MATERIAL COVERED BY THE ATOMIC ENERGY ACT

Nothing in this order shall supersede any requirements made by or under the Atomic Energy Act of August 30, 1954, as amended. "Restricted data," and material designated as "formerly restricted data," shall be handled, protected, classified, downgraded and declassified in conformity with the provisions of the Atomic Energy Act of 1954, as amended, and the regulations of the Atomic Energy Commission.

SECTION 9. SPECIAL DEPARTMENTAL ARRANGEMENTS

The originating department or other appropriate authority may impose, in conformity with the provisions of this order, special requirements with respect to access, distribution and protection of classified information and material, including those which presently relate to communications intelligence, intelligence sources and methods and cryptography.

SECTION 10. EXCEPTIONAL CASES

In an exceptional case when a person or department not authorized to classify information originates information which is believed to require classification, such person or department shall protect that information in the manner prescribed by this order. Such persons or department shall transmit the information forthwith, under appropriate safeguards, to the department having primary interest in the subject matter with a request that a determination be made as to classification.

SECTION 11. DECLASSIFICATION OF PRESIDENTIAL PAPERS

The Archivist of the United States shall have authority to review and declassify information and material which has been classified by a President, his White House staff or special committee or commission appointed by him and which the Archivist has in his custody at any archival depository, including a presidential library. Such declassification shall only be undertaken in accord with: (i) the terms of the donor's deed of gift, (ii) consultation with the departments having a primary subject-matter interest, and (iii) the provisions of section 5.

SECTION 12. HISTORICAL RESEARCH AND ACCESS BY FORMER GOVERNMENT OFFICIALS

The requirement in section 6(A) that access to classified information or material be granted only as is necessary for the performance of one's duties shall not apply to persons outside the executive branch who are engaged in historical research projects or who have previously occupied policymaking positions to which they were appointed by the President; *Provided*, however, that in each case the head of the originating department shall: (i) determine that access is clearly consistent with the interests of national security; and (ii) take appropriate steps to assure that classified information or material is not published or otherwise compromised.

Access granted a person by reason of his having previously occupied a policymaking position shall be limited to those papers which the former official originated, reviewed, signed or received while in public office.

SECTION 13. ADMINISTRATIVE AND JUDICIAL ACTION

(A) Any officer or employee of the United States who unnecessarily classifies or overclassifies information or material shall be notified that his actions are in violation of the terms of this order or of a directive of the President issued through the National Security Council. Repeated abuse of the classification process shall be grounds for an administrative reprimand. In any case where the departmental committee or the Interagency Classification Review Committee finds that unnecessary classification or overclassification has occurred, it shall make a report to the head of the department concerned in order that corrective steps may be taken.

(B) The head of each department is directed to take prompt and stringent administrative action against any officer or employee of the United States, at any level of employment, determined to have been responsible for any release or disclosure of national security information or material in a manner not authorized by or under this order or a directive of the President issued through the National Security Council. Where a violation of criminal statutes may be involved, departments will refer any such case promptly to the Department of Justice.

SECTION 14. REVOCATION OF EXECUTIVE ORDER NO. 10501

Executive Order No. 10501 of November 5, 1953, as amended by Executive Orders No. 10816 of May 8, 1959, No. 10901 of January 11, 1961, No. 10964 of September 20, 1961, No. 10985 of January 15, 1962, No. 11097 of March 6, 1963, and by section 1(a) of No. 11382 of November 28, 1967, are superseded as of the effective date of this order.

SECTION 15. EFFECTIVE DATE

This order shall become effective on June 1, 1972.

RICHARD NIXON.

MARCH 8, 1972.

THE WHITE HOUSE

ORDER

Pursuant to section 2(A) of the Executive order of March 8, 1972, entitled Classification and Declassification of National Security Information and Material, I hereby designate the following offices in the Executive Office of the President as possessing authority to originally classify information or material "top secret" as set forth in said order:

The White House Office.
National Security Council.
Office of Management and Budget.
Domestic Council.
Office of Science and Technology.
Office of Emergency Preparedness.
President's Foreign Intelligence Advisory Board.
Council on International Economic Policy.
Council of Economic Advisers.
National Aeronautics and Space Council.
Office of Telecommunications Policy.

RICHARD NIXON.

EXECUTIVE ORDER 11714

AMENDING EXECUTIVE ORDER NO. 11652 ON CLASSIFICATION AND DECLASSIFICATION OF NATIONAL SECURITY INFORMATION AND MATERIAL

By virtue of the authority vested in me by the Constitution and statutes of the United States, the second sentence of section 7(A) of Executive Order No. 11652 of March 8, 1972, is amended to read as follows:

"To assist the National Security Council, an Interagency Classification Review Committee shall be established, composed of a Chairman designated by the President, the Archivist of the United States, and representatives of the Departments of State, Defense and Justice, the Atomic Energy Commission, the Central Intelligence Agency and the National Security Council Staff."

RICHARD NIXON.

The White House,
April 24, 1973.

O